Protéger son ordinateur et sa vie privée sur Internet





La question de la sécurité de son ordinateur est de la responsabilité de chacune et chacun d'entre nous et doit être prise au sérieux…

Depuis l'arrivée d'Internet et sa démocratisation, nous sommes de plus en plus connectés. Désormais, nous pouvons surfer, depuis n'importe où et n'importe quand, à partir d'un PC, d'une tablette ou d'un smartphone, pour y faire des achats, consulter des documents administratifs, échanger avec sa famille et ses amis…

Les objets connectés ont envahi notre quotidien et se sont rendus aussi indispensables que notre bon vieil ordinateur classique.

Mais, qui dit connexion sur le réseau, dit aussi ***collecte de données personnelles*** et ***risques pour la vie privée*** :

Toutes nos connexions laissent des traces et la technologie permet désormais aux entreprises commerciales, mais également aux personnes mal intentionnées, de collecter une multitude de données privées et de connaître ce que chacun fait sur Internet.

Nos traces sur Internet… Dès que l'on se connecte pour naviguer sur Internet, on transmet des informations…



Sur notre ordinateur : Le ***navigateur Internet*** enregistre tous les sites que l'on visite, ainsi que les mots de passe dont on se sert pour y accéder.

En ligne : Notre ***fournisseur d'accès Internet (FAI)*** enregistre toutes nos actions, chaque page visitée. Les ***sites que nous visitons*** enregistrent sur notre ordinateur des ***cookies***, qui sont de petits fichiers textes contenant diverses informations, afin de savoir ce que l'on consulte et de nous reconnaître lors de la prochaine connexion.

Ces cookies peuvent rester discrets sur notre ordinateur pendant des années si l'on n'utilise pas un **outil de nettoyage** tel que **Ccleaner** qui efface les fichiers inutiles ainsi que les divers historiques.

Il est donc important de nettoyer son PC régulièrement avec Ccleaner…



Pour protéger son ordinateur et sa vie privée sur Internet

Il faut donc apprendre à :

- **Paramétrer correctement** son **ordinateur** (compte Microsoft, système d'exploitation, navigateur Internet…).
- **Paramétrer** également **les comptes d'éditeurs** dont on utilise les applications, en particulier :
  - ✓ Le compte **Google** si on utilise Chrome, Gmail, Google photo, Google+, Google contacts, Google Drive, YouTube, etc.
  - ✓ Le compte **Orange** si on utilise les applications Orange.
  - ✓ Le compte **Samsung** sur PC, mobile ou tablette Samsung si l'on utilise les applications Samsung, etc.
- **Préserver** sa **vie privée** et ses **données en ligne**.
- **Repérer les menaces** : Virus, malwares, spywares, rootkits, randsoms et autres programmes malveillants, ***et à s'en protéger…***

***Tout ordinateur, tablette, smartphone, objet connecté à un réseau informatique est potentiellement vulnérable face à une attaque*.**

Pour éviter que son PC soit infecté par des virus, malwares, spywares, rootkits, randsom, bots et les multiples autres dangers que l’on peut rencontrer sur Internet, il faut donc avoir un **ordinateur bien sécurisé**.

Afin d'arriver à ce résultat, il existe une liste (non exhaustive) d’actions préventives.

Nous allons aborder ici quelques une des précautions élémentaires à prendre pour naviguer sur Internet en relative sécurité.

La première des défenses restera toujours l'utilisateur :

Un utilisateur averti a beaucoup moins de chance de se faire berner par un des nombreux maux d'internet.

Voici quelques unes des précautions de base à prendre pour protéger son ordinateur et sa vie privée sur Internet :

- ✓ Bien **paramétrer** son compte Microsoft et les comptes d'éditeurs pour les applications et progiciels installés sur son ordinateur,
- ✓ **Mettre à jour** sa configuration (Windows update).
- ✓ **Gérer les différents services Windows** (pare feu, points de restauration…).
- ✓ Installer une bonne défense **antivirus** **ET** **antimalwares**.
- ✓ Bien définir ses **mots de passe** (utiliser **M**ajuscules, **m**inuscules, **chiffres**, **caractères spéciaux**…), les noter pour les mémoriser et **NE PAS LES ENREGISTRER DANS SON PC** (ou bien on peut utiliser un gestionnaire de mots de passe tel que KeePass ou Dashlane).
- ✓ Veiller à **sauvegarder régulièrement ses données sur un support externe (Disque dur, clé USB...).**

En plus de ces règles basiques il existe des règles de bon sens et de bonne pratique :

- ✓ **Nettoyer régulièrement son ordinateur,** avec Ccleaner par exemple.
- ✓ **Ne télécharger ses logiciels et leurs mises à jour que sur les plateformes des éditeurs.**
- ✓ **Rester très vigilant** lorsque l'on visite un site (même connu) : **attention aux faux sites.**
- ✓ **Avant de cliquer sur un lien de téléchargement** pour installer un programme, rester vigilant : **lisez bien ce qui est affiché et proposé sur l'écran** (**Case déjà cochée, à décocher**, proposant un ou plusieurs **programmes supplémentaires** inutiles, souvent nuisibles et qui ralentissent les ordinateurs).
- ✓ **Ne pas utiliser** de cracks, de patch, de keygen (générateurs de clés de licences logicielles piratées)…

Savoir configurer Windows 10 et le Sécuriser

Si vous avez récemment installé Windows 10 ou si vous avez acheté un nouvel ordinateur sur lequel est installé le dernier système d’exploitation de Microsoft, alors l’un de vos soucis est certainement de savoir comment configurer Windows 10 pour le sécuriser au mieux.

La bonne nouvelle c’est que ce système est nettement plus sécurisé que ses prédécesseurs (Windows 7 et Windows 8).

Cependant, il reste des options à ne pas oublier pour compléter le processus et vraiment se protéger des différentes menaces et attaques.

Installation de Windows 10 :
Compte local ou compte Microsoft ?

C'est la question importante que l'on doit se poser avant même d'installer Windows 10 : compte local ou compte Microsoft ?

- Compte « local » (avec un nom d'utilisateur, comme sous les précédentes versions de Windows).

- Compte Microsoft (avec une adresse de messagerie et son mot de passe).

L'utilisation d'un compte Microsoft est plus simple pour un utilisateur néophyte.

Par contre, lorsqu'on a des ordinateurs en réseau, il est préférable d'utiliser un compte local.

Le choix se fera lors de l'installation. On pourra, cependant, changer de compte ultérieurement.

Le choix est important : Avantages et inconvénients…

Type de compte	Avantages et inconvénients
Compte local	On ouvre sa session avec le nom d'utilisateur qu'on aura choisi (comme avant) On n'est pas obligé d'avoir un mot de passe. Attention, car il faudra se connecter au coup par coup avec un compte Microsoft pour accéder aux applications Microsoft : Courrier, Calendrier, Contacts et à Windows Store
Compte Microsoft	On ouvre sa session avec l'adresse mail et le mot de passe de son compte Microsoft. On est automatiquement identifié lorsqu'on utilise Windows Store ou toute autre application Microsoft : Skype, Jeux / Xbox, Courrier, Calendrier, Contacts On est automatiquement connecté à OneDrive. Le compte Microsoft est plus simple pour les utilisateurs débutants.

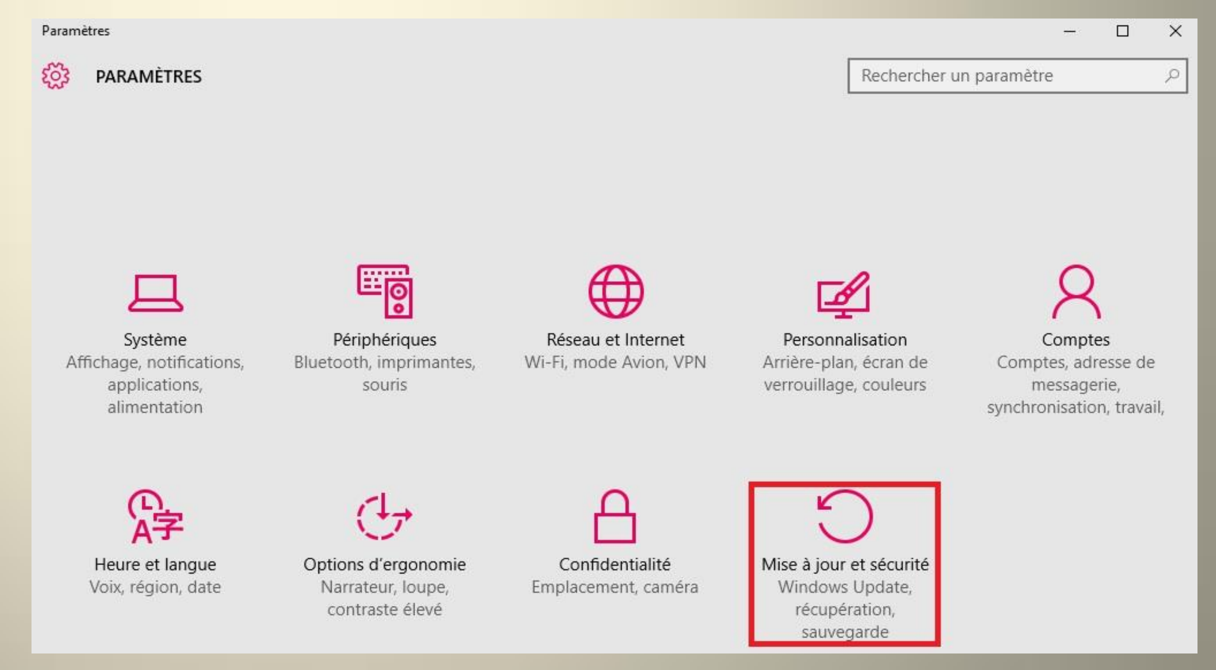
Installer les correctifs et gardez à jour votre système d’exploitation

Pour Windows l’installation des mises à jour ne pose aucune difficulté car il suffit d’activer l’installation automatique à l’aide de «Windows update» :

- Tapez «**Windows update»** dans la barre de recherche.
- Cliquez sur «**modifier les paramètres**»
- Choisissez «**Installer les mises à jour automatiquement (recommandé)»**
- De cette façon, Windows recherchera et installera automatiquement les mises à jour dès qu’elles sont lancées par Microsoft.

Cependant, un utilisateur averti peut décider de **désactiver les mises à jour automatiques** et **demander à être prévenu des mises à jour pour les déclencher lui-même :**
En effet, les mises à jour de Microsoft sont pour la plupart essentielles mais leur principal défaut, est qu'elles s'installent « furtivement » .
Ce qui peut causer des redémarrages intempestifs, susceptibles de créer des situations critiques, comme la perte de données non sauvegardées.

Pour désactiver les mises à jour automatiques et **planifier les redémarrages** il faut cliquer dans le menu « **Paramètres** », sur l'option « **Mise à jour et sécurité** ».



Dans la fenêtre qui apparaît cliquez sur « **Windows update** » puis sur « **Options avancées »** en bas de la fenêtre de droite.

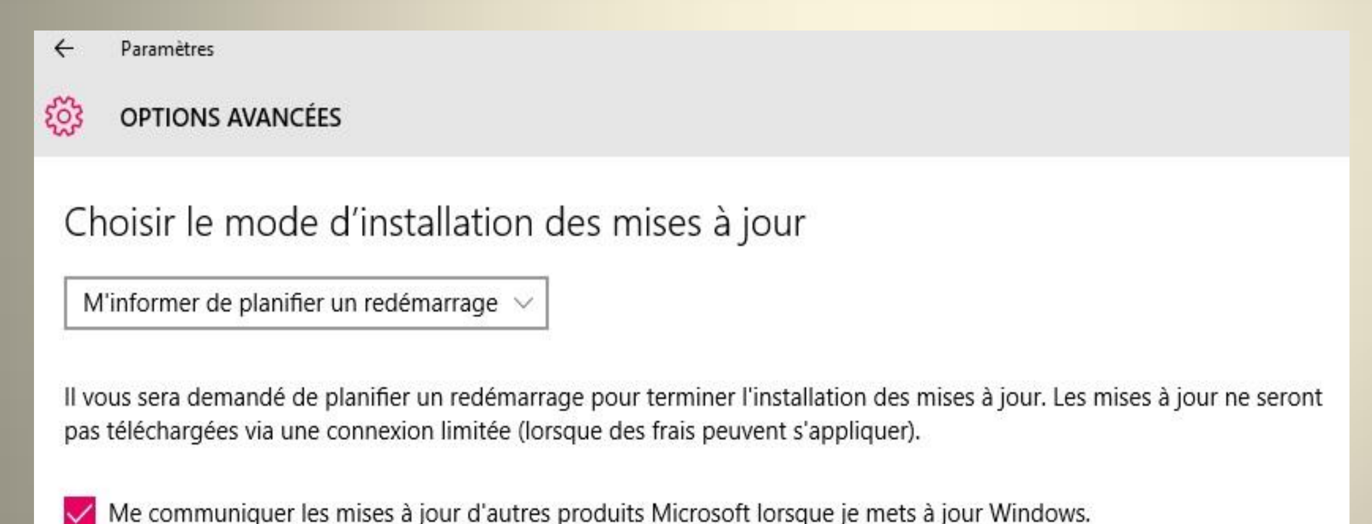
Redémarrer

Vous recherchez des informations sur les toutes dernières mises à jour ?

En savoir plus

Options avancées

Dans le menu de droite modifier l'option **« Automatique »** en **« M'informer de planifier un redémarrage »**.



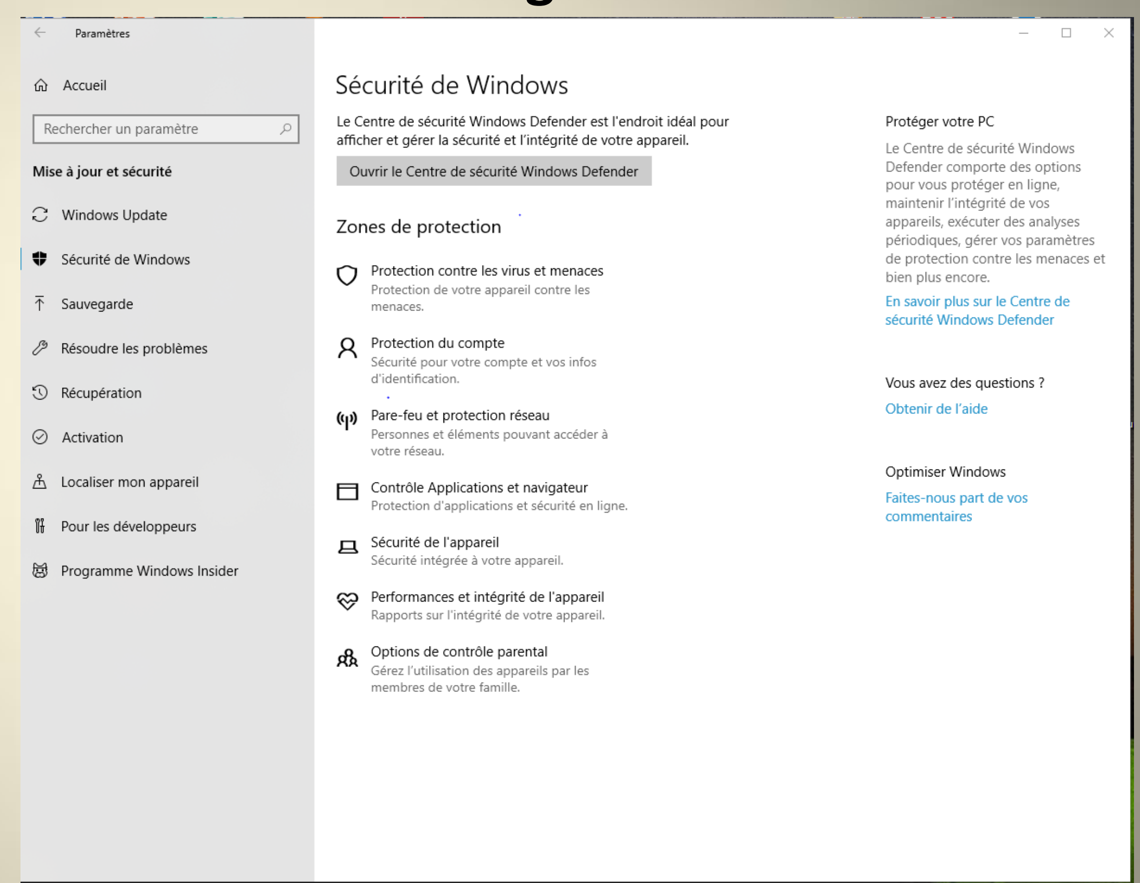
N'oubliez pas de cocher l'option **« Me communiquer les mises à jour d'autres produits Microsoft lorsque je mets à jour Windows ».**

C'est particulièrement nécessaire si vous utilisez Microsoft Office car les mises à jour de sécurité relatives aux produits Office seront également installées.

Être protégé avec « Sécurité Windows »

Windows 10 met à notre disposition une protection antivirus complète baptisée **« Sécurité Windows » qui remplace très bien n'importe quel autre suite antivirus spécialisée et bénéficie régulièrement de mises à jour.**

Lorsqu'on démarre Windows 10, **« Sécurité Windows »** est activée et protège activement notre appareil en recherchant des logiciels malveillants, des virus et toutes menaces à la sécurité de notre PC.



<u>**Remarque**</u> : Dans les versions précédentes de Windows 10, **« Sécurité Windows » est appelée « Centre de sécurité Windows Defender »**.

Rester protégé avec « Sécurité Windows »

Avec la protection en temps réel, **« Sécurité Windows »** analyse nos téléchargements et les programmes que l'on exécute sur notre PC.

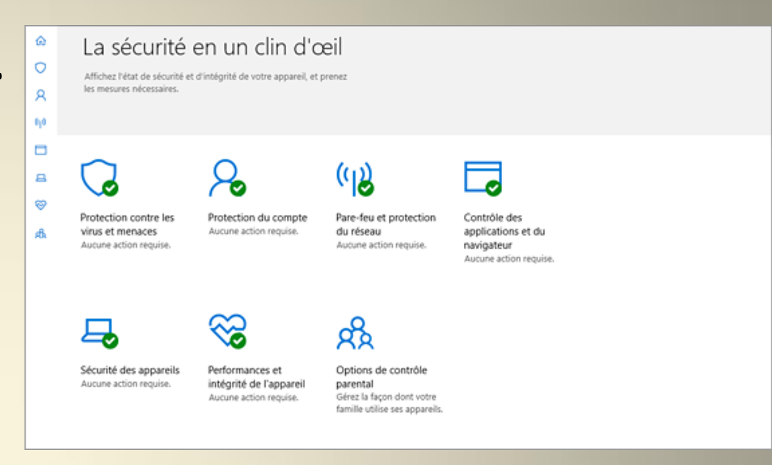
En outre, **« Windows Update »** télécharge automatiquement les mises à jour de **« Sécurité Windows »** pour nous aider à sécuriser notre ordinateur et à le protéger contre les menaces.

« Sécurité Windows » met à notre disposition les mises à jour de la protection antivirus en nous indiquant quand :

- ✓ notre appareil a été analysé contre les menaces la dernière fois ;
- ✓ nos définitions **antivirales** ont été mises à jour la dernière fois ; *(Les définitions sont des fichiers que le logiciel **« Sécurité Windows »** utilisent pour protéger notre PC contre les menaces les plus récentes)* ;
- ✓ l'analyse de performances et d'intégrité de l'appareil a été exécutée pour garantir le fonctionnement efficace de votre ordinateur.

Remarque : Si vous installez une autre application antivirus, **« Sécurité Windows »** est automatiquement désactivée.

« Sécurité de Windows » comporte sept zones qui protègent votre appareil et vous permettent de spécifier la manière dont votre appareil est protégé :



- ✓ **Protection contre les virus et menaces.**
- ✓ **Protection du compte**.
- ✓ **Pare-feu et protection réseau**.
- ✓ **Contrôle Applications et navigateur**.
- ✓ **Sécurité de l'appareil.**
- ✓ **Performances et intégrité de l'appareil**.
- ✓ **Options de contrôle parental**.

Vous verrez que certaines de ces zones affichent une icône de statut :

- ✓ **Vert** signifie que votre appareil est suffisamment protégé et qu'aucune action n'est recommandée.
- ✓ **Jaune** indique qu'une recommandation de sécurité est disponible.
- ✓ **Rouge** vous alerte lorsqu'un événement requiert votre attention immédiate.

Activer le pare feu de Windows 10 :

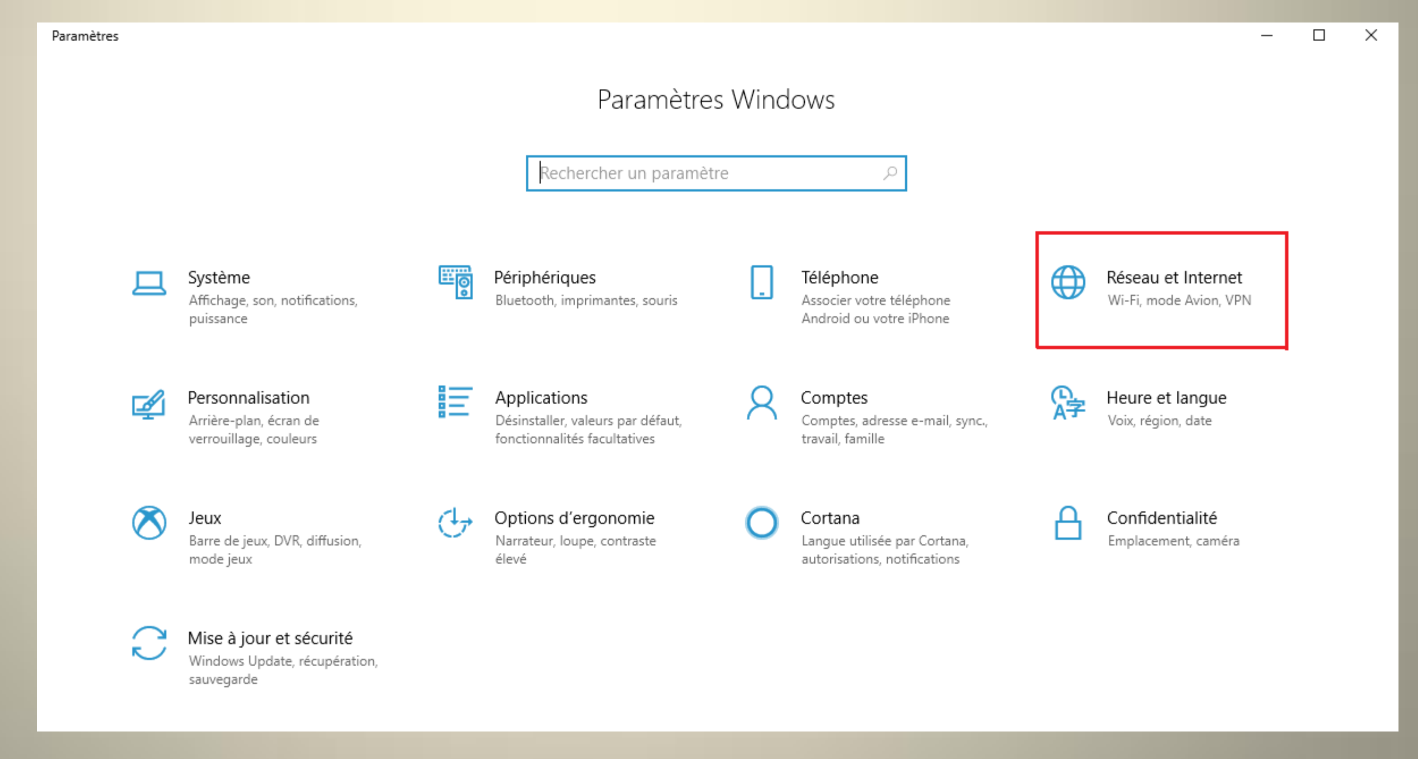
Le pare feu de Windows est très efficace.

Il permet de connaitre avec précision les programmes qui communiquent avec les différents réseaux auxquels vous adhérez.

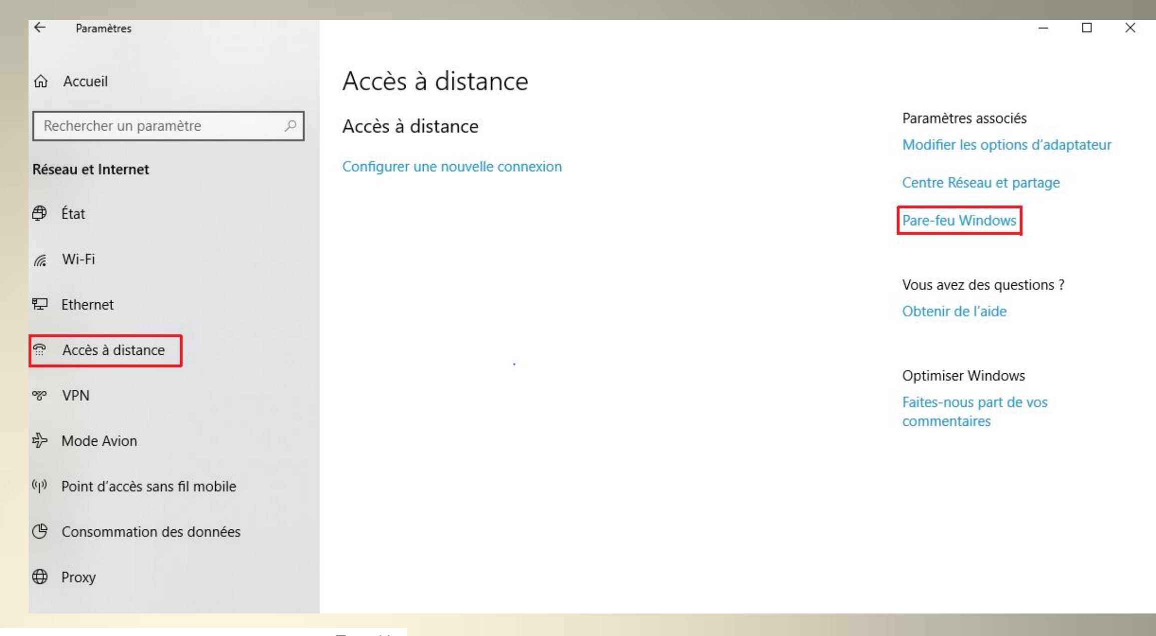
Pour cela, il est nécessaire de bien configurer le pare feu Windows 10.

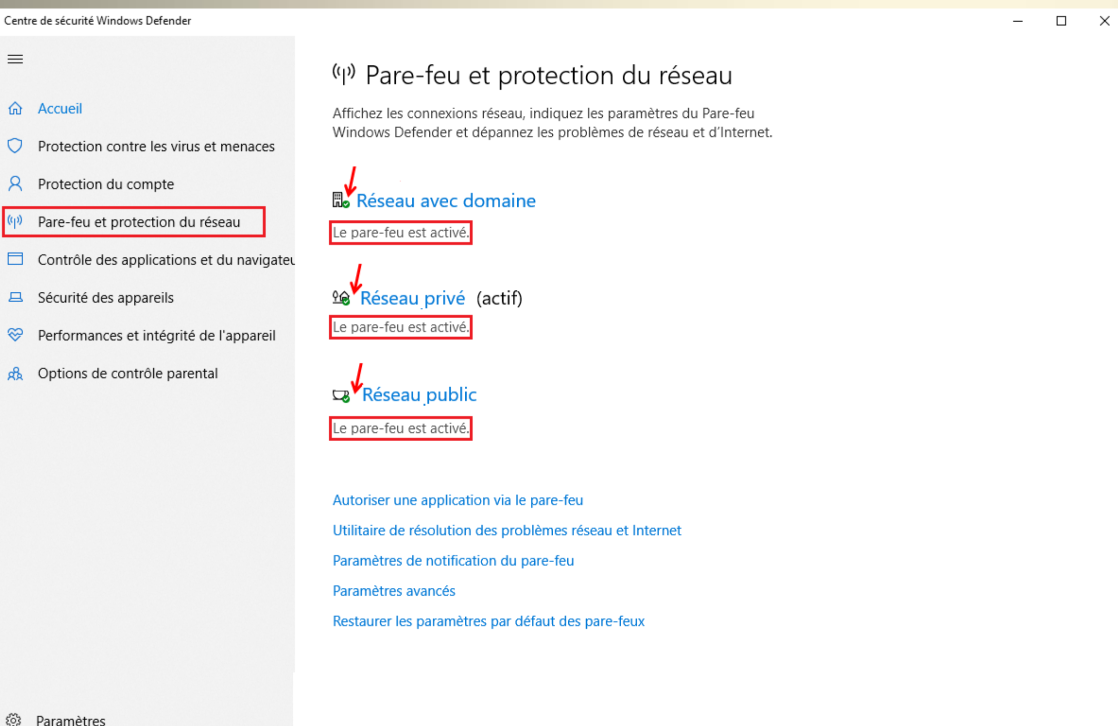
Pour activer le pare feu :

Dans la fenêtre des « **Paramètres** » cliquer sur l'option « **Réseau et internet** » :



Dans la fenêtre qui apparaît cliquer sur l'onglet « **Accès à distance** » puis sur l'option « **Pare feu et protection du réseau** ».





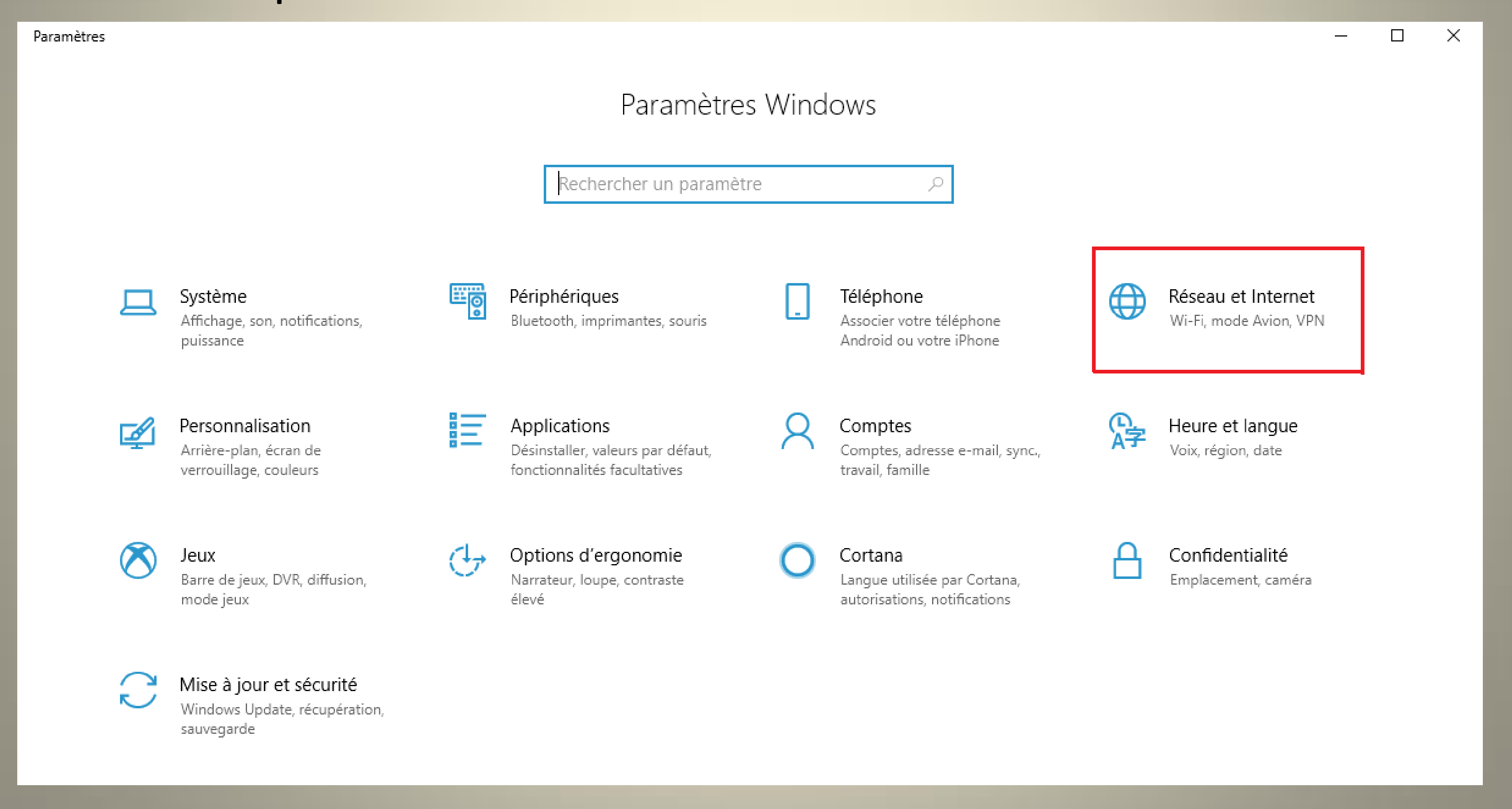
Le pare feu Windows 10 s'ouvre.

Si la couleur affichée est **verte** c'est qu'il est activé sinon vous devrez l'activer en cliquant sur chaque type de réseau (domaine, privé et public) et l'activer.

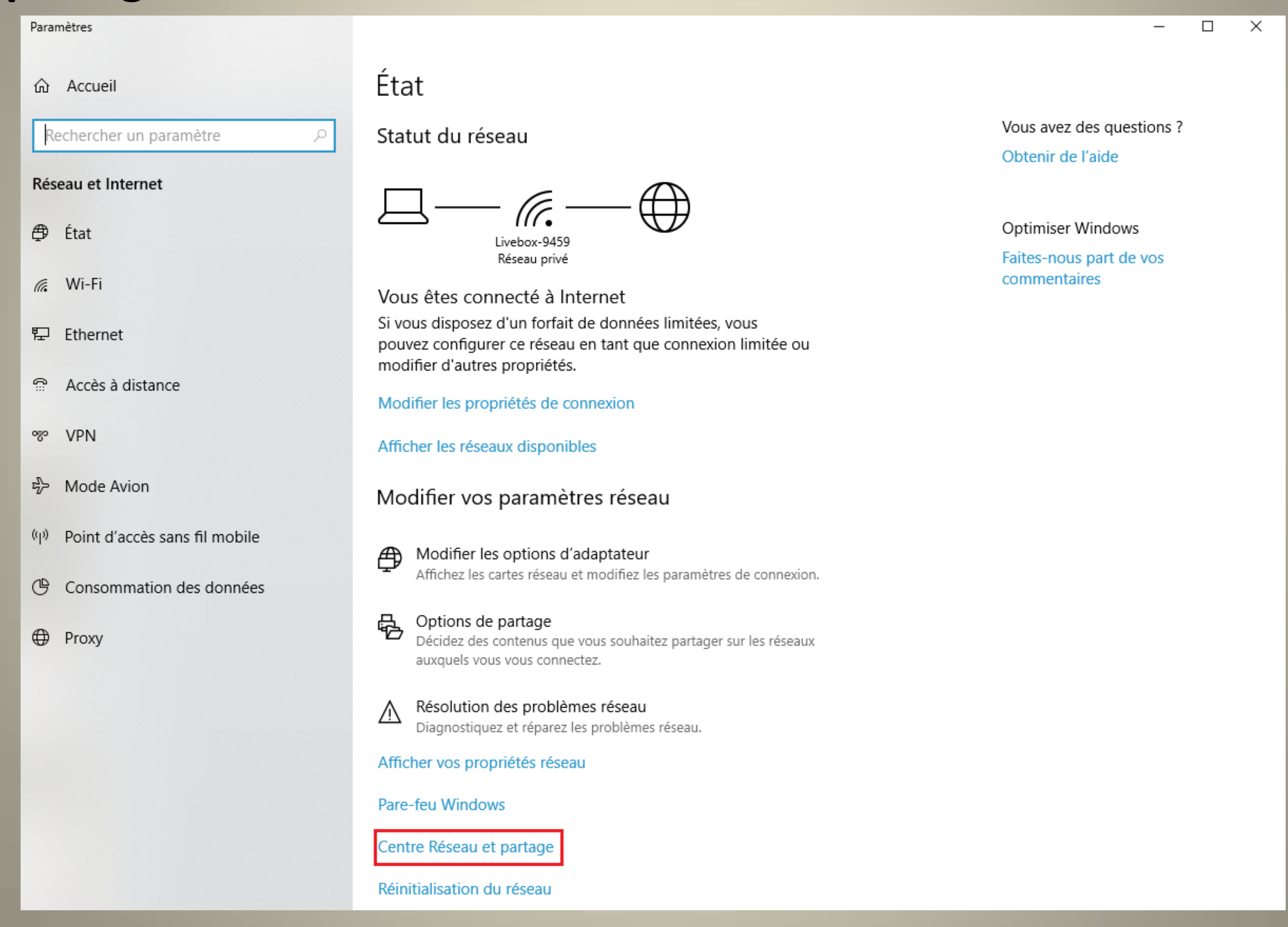
Configurer le partage de fichiers

Lorsque vous êtes connecté sur un réseau, il est préférable de bien configurer les options du partage avancé.

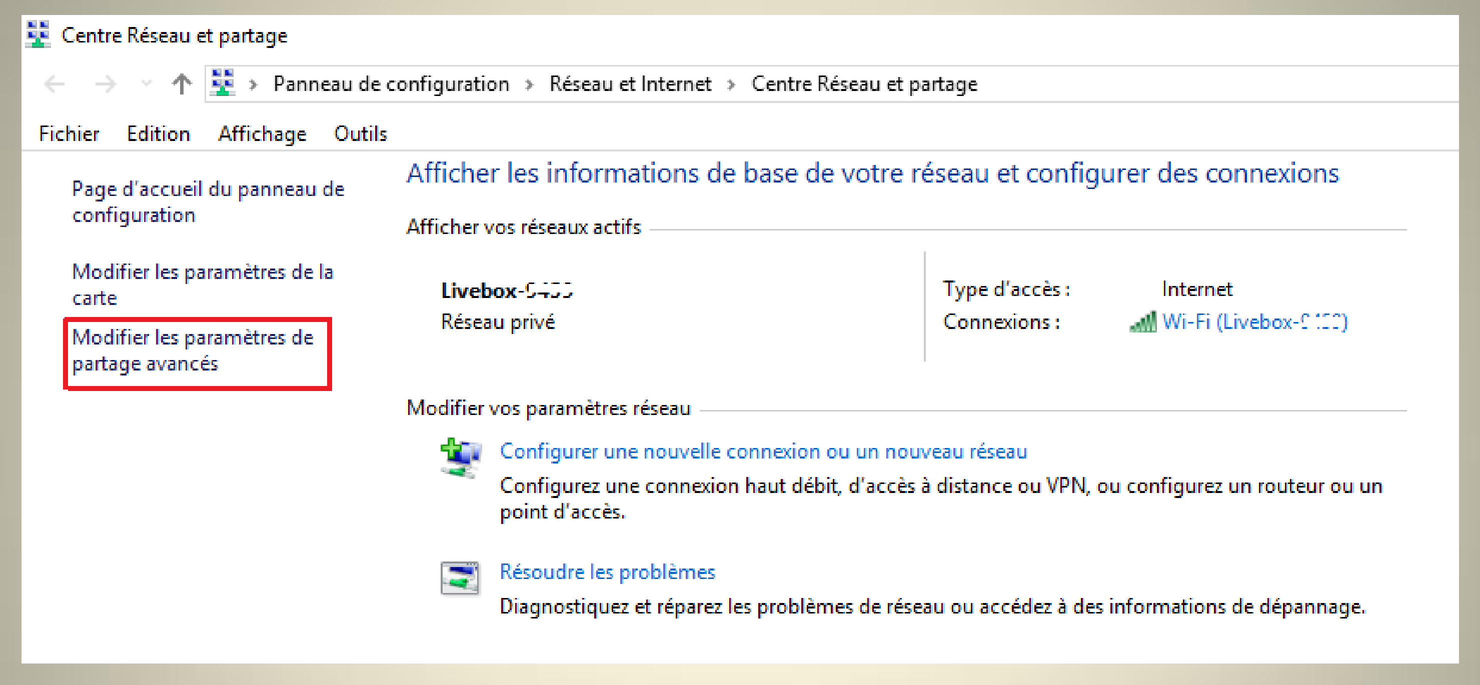
Pour y accéder, cliquez sur l'option **« Réseau et internet »** dans la fenêtre des paramètres :



Dans l'interface qui s'affiche, cliquez sur l'option **« Centre Réseau et partage »** :



Le Centre réseau et partage s’affiche. Pour accéder aux options du partage avancé cliquez sur l’option « **Modifier les paramètres de partage avancé** » :



Dans la fenêtre qui apparaît, vous pouvez configurer les options de partage avancées.

Vous avez accès à 3 catégories : Privé, Invité ou Public et tous les réseaux :

Pour la catégorie « **Privé** » :

Modifier les options de partage pour d'autres profils réseau

Windows crée un profil réseau distinct pour chaque réseau utilisé. Vous pouvez choisir des options spécifiques pour chaque profil.

Privé (profil actuel)

Recherche du réseau

Quand la découverte du réseau est activée, cet ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau.

- (•) Activer la découverte de réseau
  - [x] Activez la configuration automatique des périphériques connectés au réseau.
- ( ) Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- (•) Activer le partage de fichiers et d'imprimantes
- ( ) Désactiver le partage de fichiers et d'imprimantes

Invité ou public

Tous les réseaux

Modifier les options de partage pour d'autres profils réseau

Windows crée un profil réseau distinct pour chaque réseau utilisé. Vous pouvez choisir des options spécifiques pour chaque profil.

Privé (profil actuel)

Invité ou public

Recherche du réseau

Quand la découverte du réseau est activée, cet ordinateur peut voir les autres ordinateurs et périphériques du réseau, et peut lui-même être vu par les autres ordinateurs du réseau.

- (•) Activer la découverte de réseau
- ( ) Désactiver la découverte de réseau

Partage de fichiers et d'imprimantes

Lorsque le partage de fichiers et d'imprimantes est activé, toute personne sur le réseau peut accéder aux fichiers et aux imprimantes que vous avez partagés à partir de cet ordinateur.

- (•) Activer le partage de fichiers et d'imprimantes
- ( ) Désactiver le partage de fichiers et d'imprimantes

Tous les réseaux

Pour la catégorie « **Invité ou Public** » :

Pour la catégorie « **Tous les réseaux** » :

Tous les réseaux

Partage de dossiers publics

Lorsque le partage des dossiers Public est activé, les utilisateurs du réseau, y compris les membres du groupe résidentiel, peuvent accéder aux fichiers des dossiers Public.

- ○ Activer le partage afin que toute personne avec un accès réseau puisse lire et écrire des fichiers dans les dossiers Public
- ◉ Désactiver le partage des dossiers Public (les personnes connectées à cet ordinateur peuvent continuer d'accéder à ces dossiers)

Diffusion de contenu multimédia

Lorsque la diffusion de contenu multimédia est activée, les utilisateurs et périphériques du réseau peuvent accéder à la musique, aux images et aux vidéos sur cet ordinateur. Ce dernier peut également trouver des fichiers multimédias sur le réseau.

Choisir les options de diffusion de contenu multimédia...

Connexions de partage de fichiers

Windows utilise le chiffrement 128 bits pour mieux protéger les connexions de partage de fichiers. Certains périphériques ne prennent pas en charge le chiffrement 128 bits et doivent utiliser le chiffrement 40 ou 56 bits.

- ◉ Utiliser le chiffrement 128 bits pour mieux protéger les connexions de partage de fichiers (recommandé)
- ○ Activer le partage de fichiers pour les périphériques qui utilisent le chiffrement 40 ou 56 bits

Partage protégé par mot de passe

Lorsque le partage protégé par mot de passe est activé, seules les personnes disposant d'un compte d'utilisateur et d'un mot de passe sur cet ordinateur peuvent accéder aux fichiers partagés, aux imprimantes connectées à l'ordinateur et aux dossiers publics. Pour donner accès à d'autres personnes, vous devez désactiver le partage protégé par mot de passe.

- ◉ Activer le partage protégé par mot de passe
- ○ Désactiver le partage protégé par mot de passe

Configurer le contrôle de compte utilisateur UAC

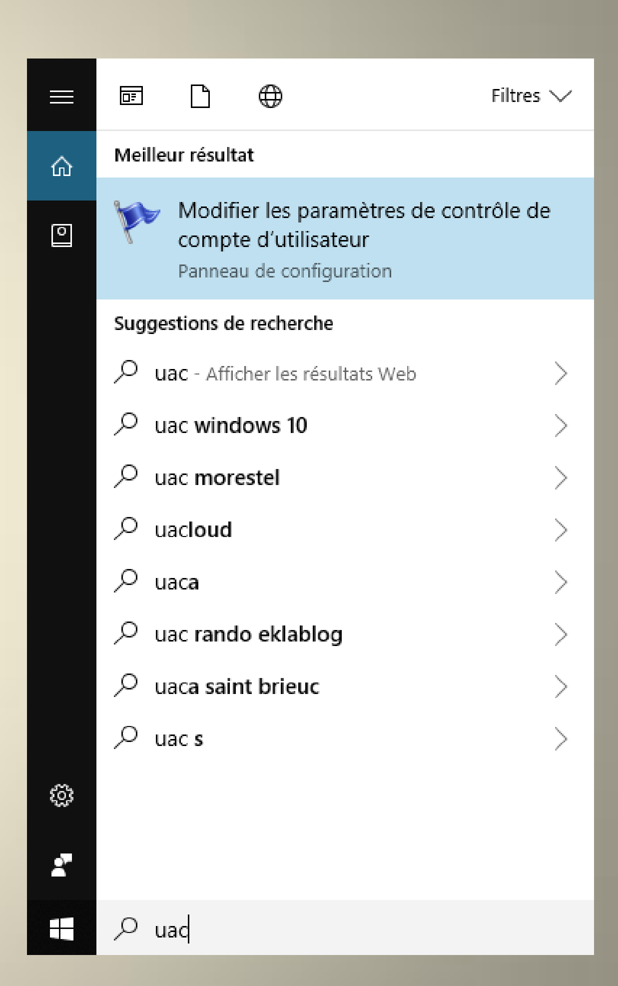
(User Account Control ou Contrôle du Compte d'Utilisateur)

Cette option est omniprésente dans Windows et cela depuis les premières versions de ce système. Elle permet de contrôler les modifications non autorisées sur votre ordinateur.

Ces modifications sont effectuées par des **applications tierces** et **peuvent influencer la sécurité de votre système**.

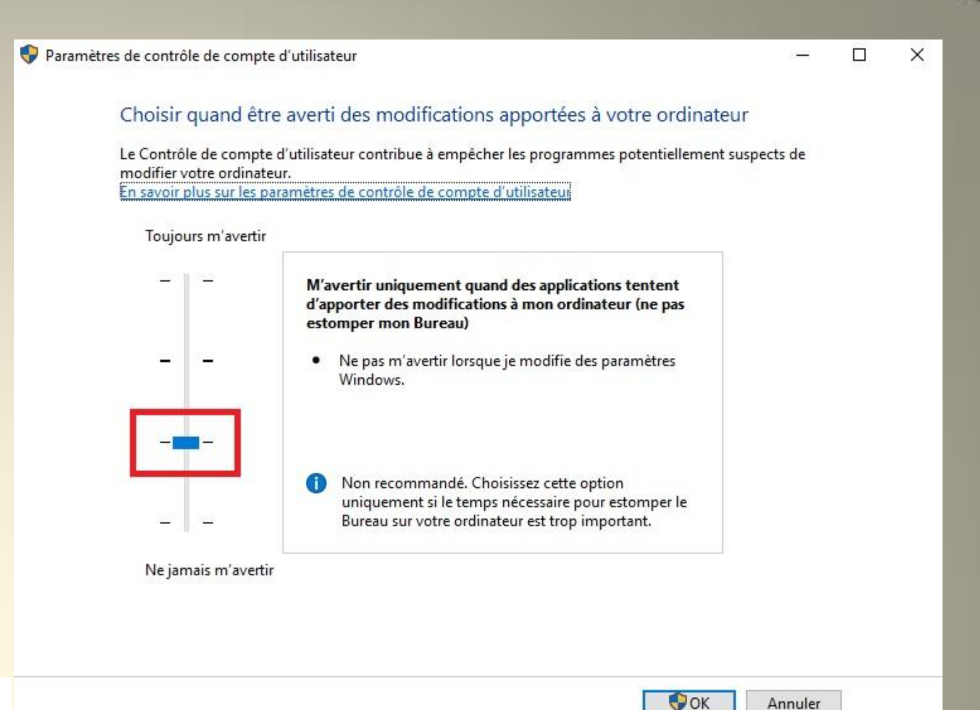
Pour accéder à l'interface du contrôle de compte utilisateur, il faut procéder comme suit :

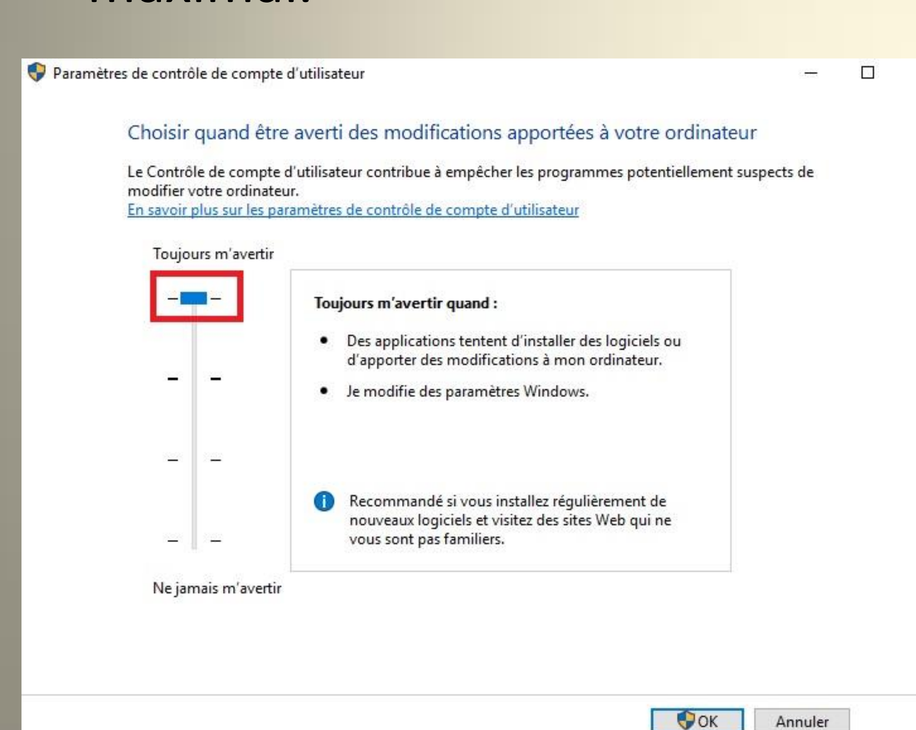
Dans la zone de recherche de la barre de menu saisissez le mot **« UAC »** puis cliquez sur le raccourci qui s'affiche.



Dans l'interface qui apparaît, on voit que la valeur par défaut est à la 2ème position.

Pour une sécurité optimale, configurer l'UAC au niveau maximal.





Ce niveau de contrôle avertit à chaque modification que peut apporter une application web, un site internet ou un logiciel qui voudrait s'installer « furtivement » sur le PC.

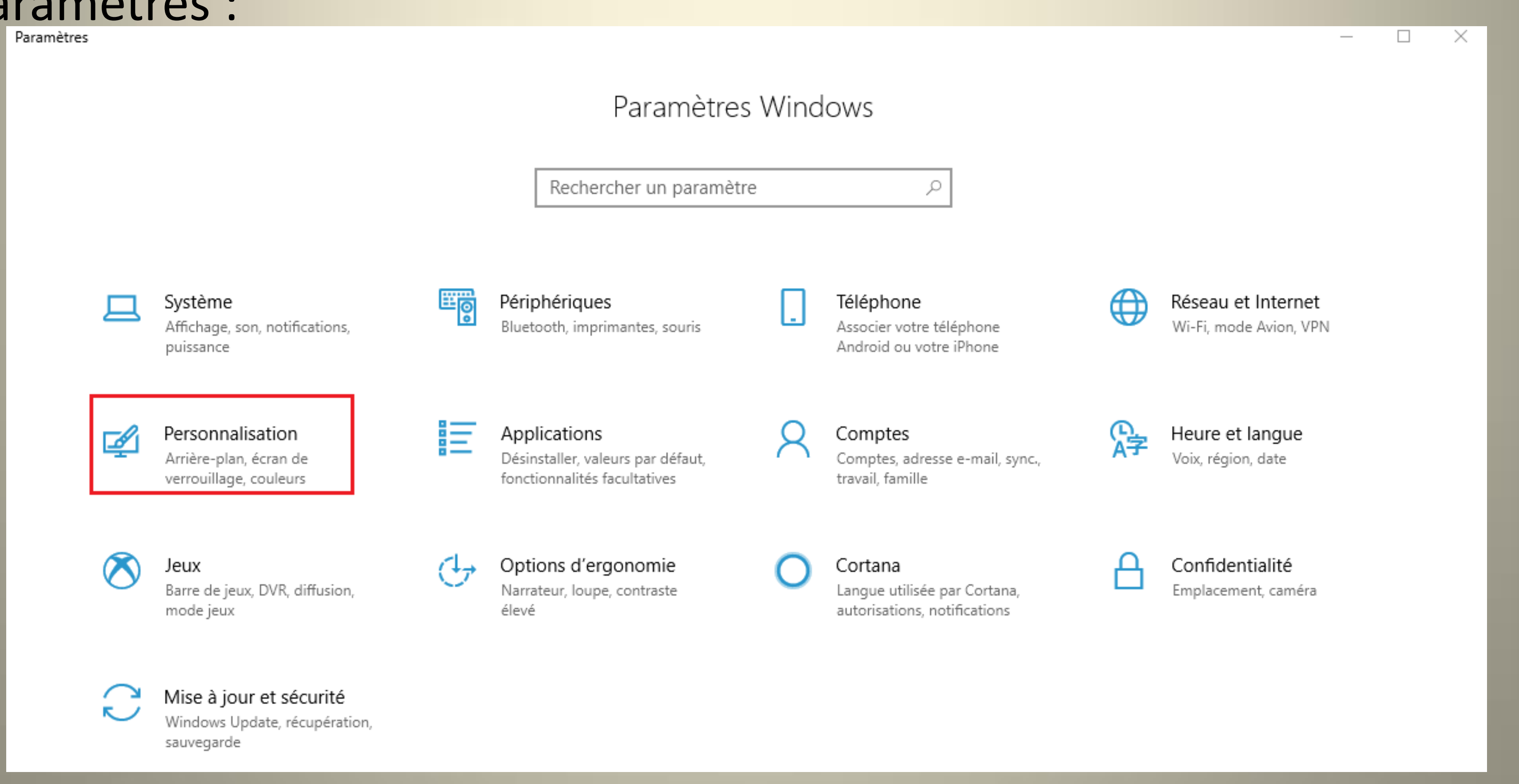
Utiliser un écran de verrouillage/déverrouillage

Pour sécuriser Windows 10, vous devez être sur que votre ordinateur est sécurisé même en votre absence.

C'est l'utilité d'un écran de verrouillage.

Pour y accéder vous devez :

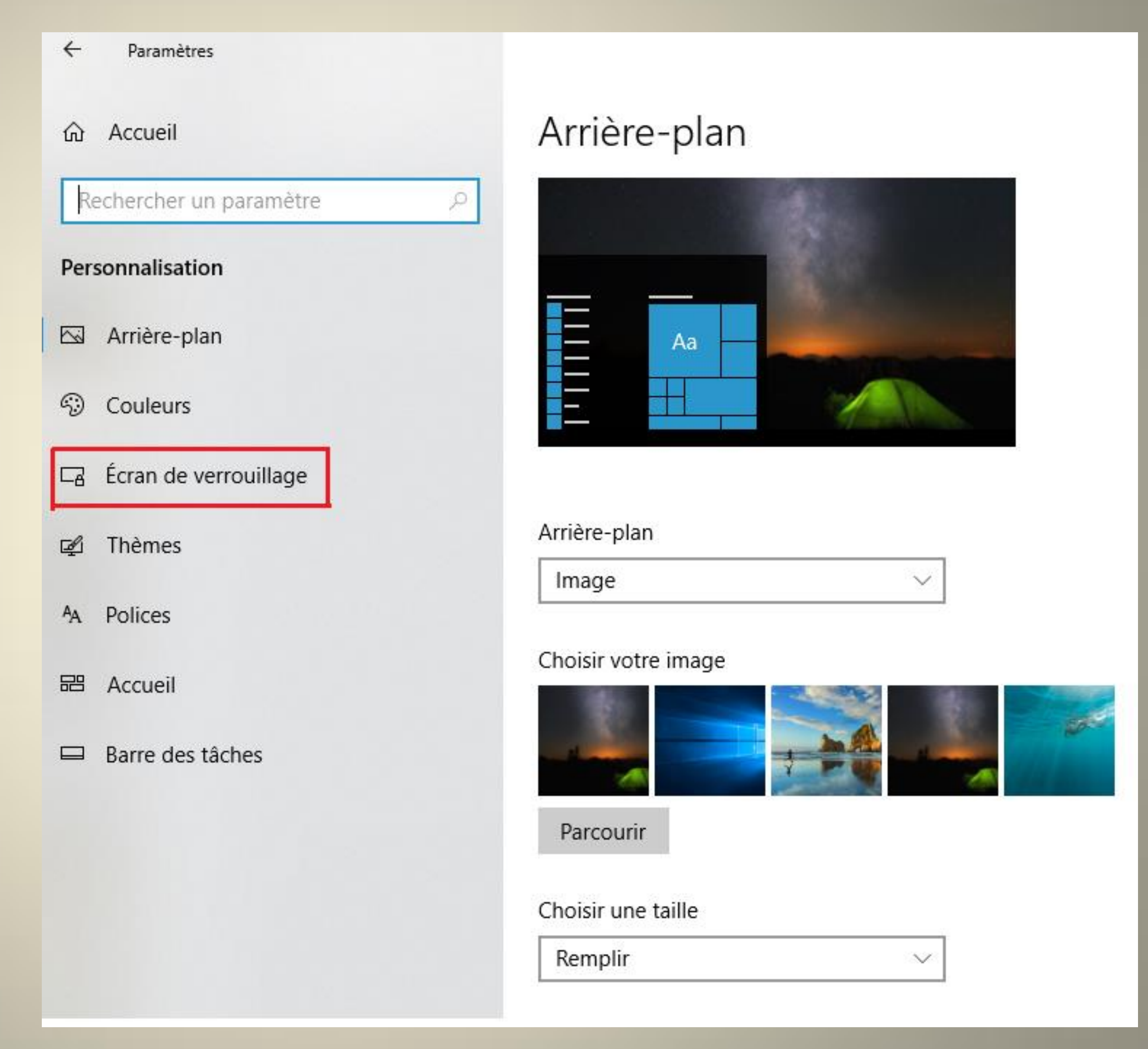
Cliquez sur la rubrique « **Personnalisation** » dans la fenêtre des paramètres :



Dans l’interface qui apparaît, cliquez sur l’option **« Écran de verrouillage »** :

Vous pouvez configurer votre écran de verrouillage comme bon vous semble selon les options disponibles.

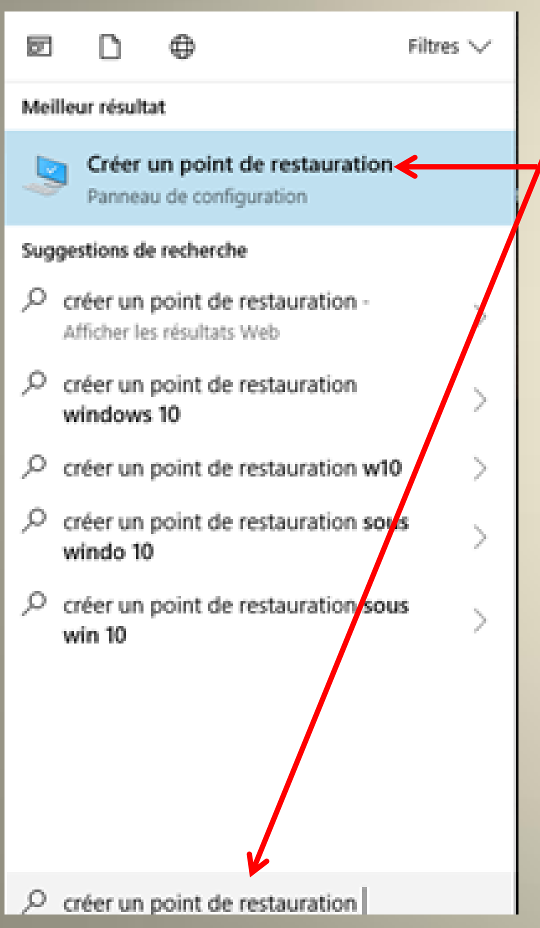
Et surtout choisissez bien les applications qui seront affichées à l’écran.



Créer un point de restauration système sous Windows 10

À Quoi Sert Un Point De Restauration Sur Windows 10 ?

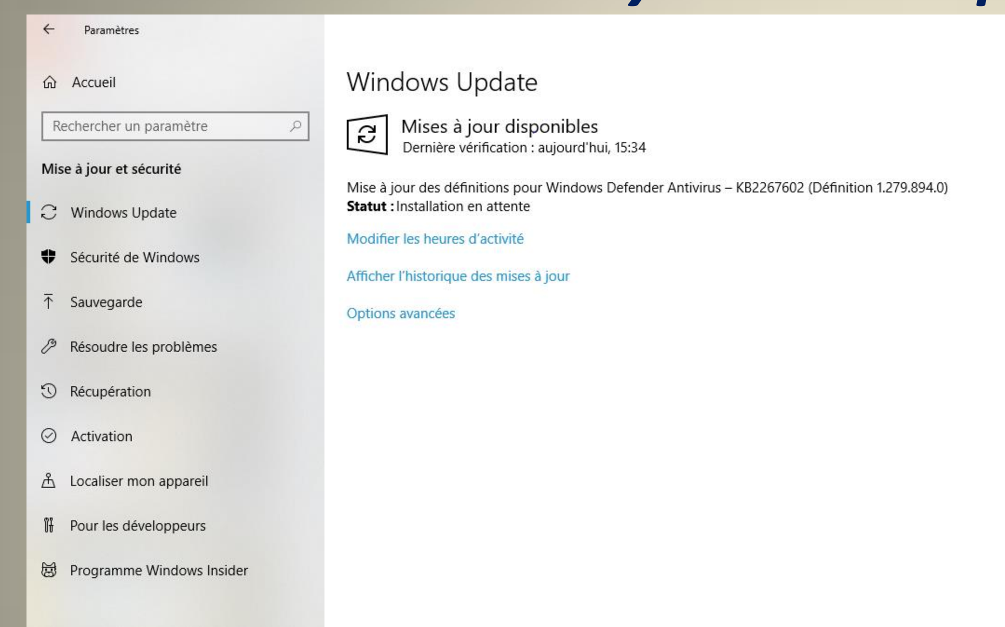
*Créer un **point de restauration Windows 10** ou encore **une image système** permet de sauvegarder l'état stable de votre système et de le récupérer en cas de besoin (panne ou irrégularité de fonctionnement de votre système).*



- ✓ Saisir « **Créer un point de restauration** » dans la fenêtre en bas à gauche, dans la barre des tâches, puis sélectionnez l'entrée dans la liste des résultats.
- ✓ Dans l'onglet **Paramètres de protection** des **Propriétés système,** sélectionnez **Créer.**
- ✓ Entrez une description (ex. point de restauration du 01/10/2018) pour le point de restauration, puis sélectionnez **Créer** > **OK.**



Installer les correctifs Windows et gardez à jour son système d’exploitation



Il faut régulièrement s’assurer que le système Windows tourne avec les dernières mises à jour de sécurité et correctifs disponibles. Les mises à jour servent à **réparer les failles de sécurité découvertes par les pirates**, à améliorer le rendement du système.

Les développeurs lancent couramment des mises à jour de leurs programmes pour **corriger les failles, les anomalies de fonctionnement et autres bugs du système d’exploitation et des applications rattachées.**

Installer les dernières mises à jour pour l'ensemble de vos programmes

Les **pirates** développent **constamment** de **nouveaux logiciels malveillants**, afin d'exploiter les vulnérabilités des programmes installés sur nos machines et ainsi attaquer ou pénétrer dans nos ordinateurs.

Donc, il ne sert à rien de mettre à jour le système d'exploitation si on ne le fait pas aussi **pour tous les autres programmes installés**.

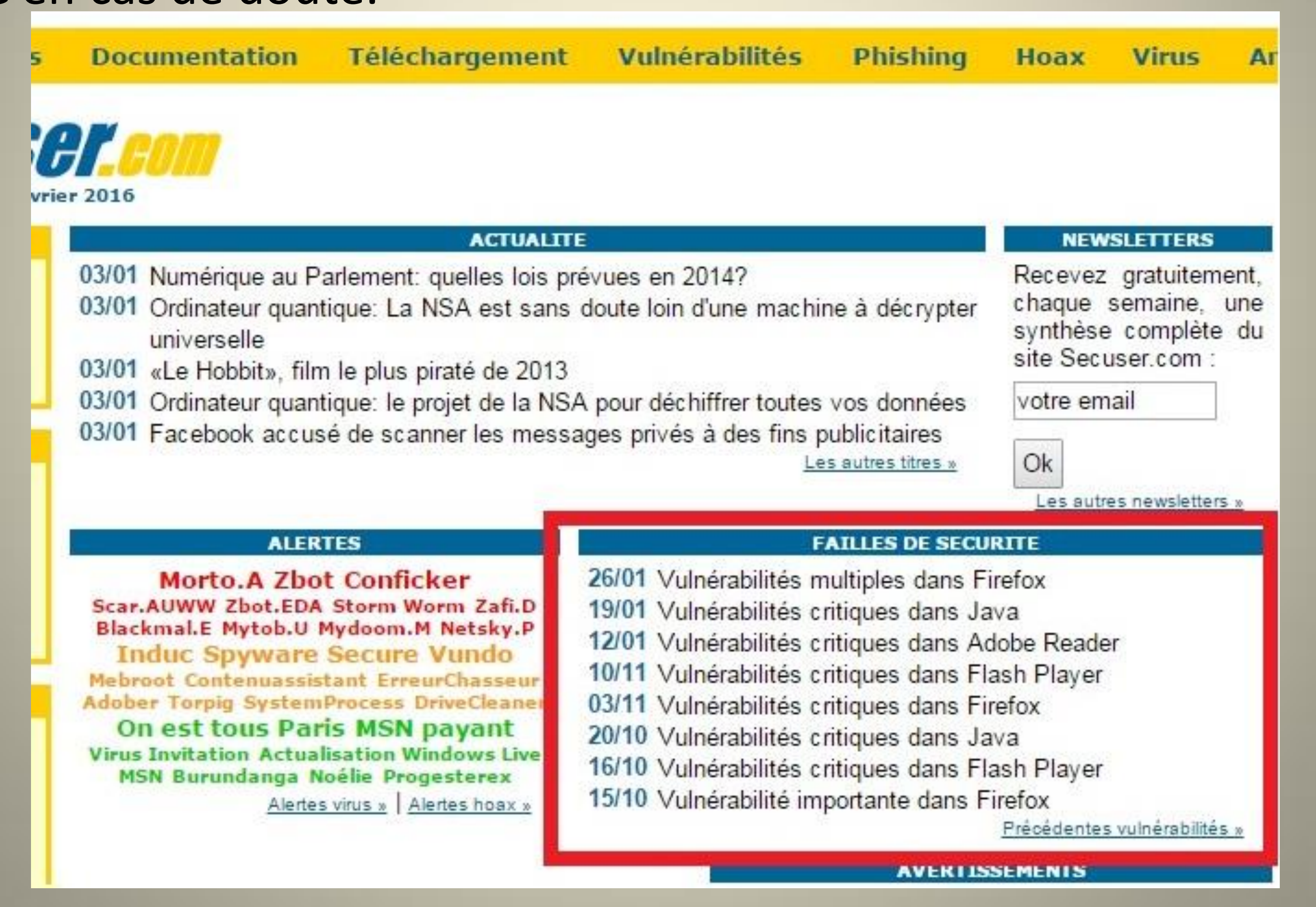
Il n'existe pas de moyen global pour installer les mises à jour automatiquement pour l'ensemble des logiciels de votre ordinateur.

Certains éditeurs de logiciels alertent lorsqu'ils diffusent leurs mises à jour mais d'autres ne le font pas.

Il est alors nécessaire de rechercher régulièrement par soi-même les mises à jour sur les sites officiels des logiciels.

Information sur les dernières menaces sur Internet

Un site (Français) : http://www.secuser.com/ permet de **consulter les dernières failles de sécurité,** voire de **lancer un scan de sécurité** sur son PC en cas de doute.



Sécurité de vos données : Réagir face à une « attaque »

Une attaque, qu'est-ce que c'est ? C'est l'exploitation d'une faille d'un système informatique **(système d'exploitation, logiciel ou bien même de l'utilisateur)** à des fins non connues par l'exploitant du système et généralement préjudiciables.



Quelles sont les méthodes de piratage et les menaces les plus courantes ?

Phishing, rançongiciels, vols de mots de passe, logiciels malveillants, faux sites internet, faux réseaux wifi… Les pirates ne manquent pas d'imagination pour tenter de s'en prendre à vos données. Voici leurs principales méthodes et des conseils simples pour vous protéger.

Le phishing

Le phishing, qu'est-ce que c'est ?

Le phishing ou hameçonnage consiste à faire croire à la victime qu'elle communique avec un tiers de confiance dans le but de lui soutirer des informations personnelles telles que son numéro de carte bancaire ou son mot de passe.

Comment vous protéger contre le phishing ?

Quelques conseils pour vous protéger contre le phishing :

- Si vous réglez un achat, vérifiez que vous le faites sur un site web sécurisé dont l'adresse commence par **« https ».**
- Si un courriel vous semble douteux, **ne cliquez pas sur les pièces jointes** ou **sur les liens qu'il contient !** Connectez-vous en saisissant l'adresse officielle dans la barre d'adresse de votre navigateur.
- **Ne communiquez jamais votre mot de passe. Aucun site web fiable ne vous le redemandera !**
- Vérifiez que votre antivirus est à jour pour maximiser sa protection contre les programmes malveillants.

Exemples de phishing



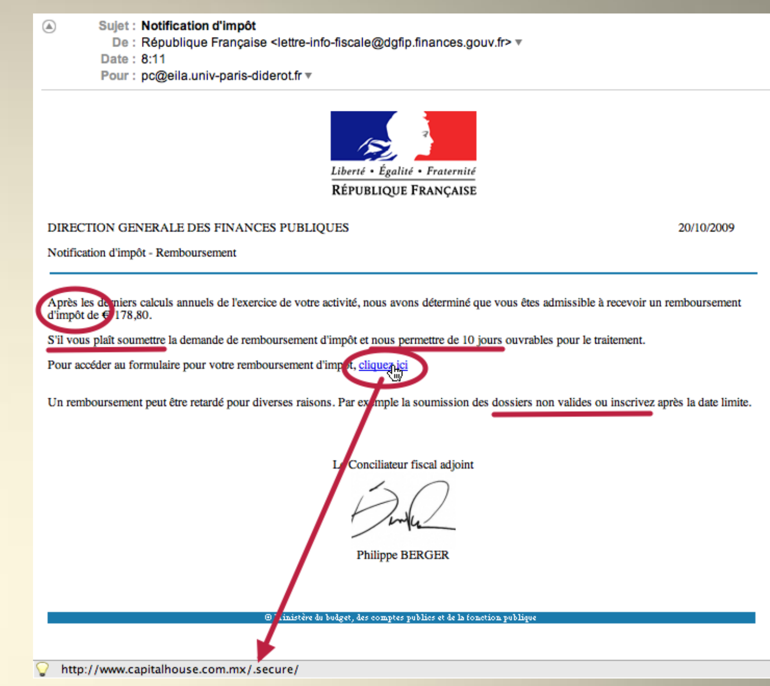
Le test du nouveau systeme de securite. Notre devise: Banking sans fraude.

Compte tenu d'accidents tres frequents provoques par des activites frauduleuses sur Internet, notre banque a introduit le nouveau systeme de securite de nos clients. Conformement a celui-la chaque mois vous serez le destinataire d'une lettre confirmante vos donnee secretes. Nous esperons votre comprehension a l'egard de cet innovation. Les mesures entreprises nous permettront de reduire les risques d'acces non sanctionne de tierces personnes a votre compte personnel, ainsi que controler l'activite de votre compte en comparant l'adresse IP et version de votre navigateur de votre session presente et celle precedente. A l'avis de l'organisation mondiale bancaire ces mesures permettront de diminuer au maximum les voles d'argent des clients.

Log in: lecreditlyonnais

Si vous n'etes pas d'accord ou mecontent de cet innovation veuillez nous ecrire a
lecreditlyonnais@banksecurity.fr
votre opinion sera prise en compte.

Nous vous remercions de nous avoir accorde vote temps et prions d'accepter nos salutations distinguees.



Sujet : Notification d'impôt
De : République Française <lettre-info-fiscale@dgfip.finances.gouv.fr>
Date : 8:11
Pour : pc@eila.univ-paris-diderot.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES — 20/10/2009

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez ici

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Le Conciliateur fiscal adjoint

Philippe BERGER

© Ministère du budget, des comptes publics et de la fonction publique

http://www.capitalhouse.com.mx/.secure/



Bleu Ciel d'EDF espaces@edf.fr via vh31.hoster.by — 4:49 AM (4 hours ago)
to me

Cher(e) Client(e),

Nous avons constatés un impayé sur votre dernière facture.

Afin de régulariser votre situation veuillez vous refferez ci-dessous :

Résoudre ce problème maintenant >

Lors d'échec de régularisation de votre situation , nous procèderons à la suspension de votre fourniture d'énergie. Cette intervention vous sera facturée.

Cordialement,

Ce message est strictement confidentiel. Son intégrité n'est pas assurée sur Internet. Si vous n'êtes pas destinataire du message, merci de le détruire. Ce message vous a été envoyé par un automate. Pour toute correspondance avec votre conseiller EDF Bleu Ciel, connectez-vous à votre espace Client. Si vous ne souhaitez plus recevoir d'autres courriers électroniques de notre part.

EDF SA au capital de 924 433 331 Euros. N°552 081 317 RCS Paris. Siège social 22-30 av de Wagram, 75382 Paris Cedex 08. Copyright EDF 2012

L'énergie est notre avenir, économisons-la !

Le rançongiciel

Qu’est-ce qu'un rançongiciel ?

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Wannacrypt, Jaff, Locky, TeslaCrypt, Cryptolocker, etc.). L’objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Comment vous protéger contre un rançongiciel ?

Trois conseils pour vous protéger contre un rançongiciel :

- Effectuez des sauvegardes régulières de vos données.
- N’ouvrez pas les messages dont la provenance ou la forme est douteuse.
- Apprenez à identifier les extensions douteuses des fichiers : si elles ne correspondent pas à ce que vous avez l’habitude d’ouvrir, ne cliquez pas ! Exemple : Vacances_photos.**exe**

Le vol de mot de passe

Le vol de mot de passe, qu’est-ce que c’est ?

Le vol de mot de passe consiste à utiliser des logiciels destinés à tenter un maximum de combinaisons possibles dans le but de trouver votre mot de passe. Le vol de mot de passe peut également se faire en multipliant les essais d’après des informations obtenues par exemple sur les réseaux sociaux.

Comment vous protéger contre un vol de mot de passe ?

Quatre conseils pour vous protéger contre un rançongiciel :

- N’utilisez pas le nom de vos enfants, de vos mascottes ou d’autres éléments susceptibles de figurer dans vos réseaux sociaux comme mot de passe.
- Construisez des mots de passe compliqués : utilisez des lettres, des majuscules et des caractères spéciaux.
- N’utilisez pas le même mot de passe partout !
- Procurez-vous un anti-virus et anti-spyware et mettez-le régulièrement à jour.

Les logiciels malveillants

Un logiciel malveillant, ou maliciel (en anglais : **malware**), **qu'est-ce que c'est ?**

Il s'agit d'un programme développé dans le seul but de nuire à un système informatique. Il peut être caché dans des logiciels de téléchargement gratuits ou dans une clé USB.

Comment vous protéger contre un logiciel malveillant ?

Deux conseils pour vous protéger contre un logiciel malveillant :

- ➢ N'installez que des logiciels provenant de sources fiables ! Si un logiciel normalement payant vous est proposé à titre gratuit, redoublez de vigilance. Préférez les sources officielles !
- ➢ Ne connectez pas une clé USB trouvée par hasard, elle est peut être piégée !

Les faux sites internet

Un faux site internet, qu'est-ce que c'est ?

Des faux sites (boutiques en ligne, sites web administratifs…) peuvent être des copies parfaites de l'original.

Leur but : récupérer vos données de paiement ou mots de passe.

Comment vous protéger contre un faux site internet ?

Encore une fois, ne saisissez pas vos données de paiement ou mots de passe dans des sites web non sécurisés, c'est-à-dire ne commençant pas par **« https ».**

Les faux réseaux wifi

Un faux réseau wifi, qu'est-ce que c'est ?

Lorsque vous êtes dans un lieu public, une multitude de connexions wifi ouvertes peuvent apparaître. Méfiez-vous, certains de ces réseaux sont piégés et destinés à voler vos informations.

Comment vous protéger contre un faux réseau wifi ?

Quatre conseils pour vous protéger contre un faux réseau wifi :

- Assurez-vous de l'originalité du réseau concerné. Si possible, demandez confirmation à l'un des responsables du réseau ouvert (Exemple : le bibliothécaire, le responsable d'un café…).
- Si vous devez créer un mot de passe dédié, n'utilisez pas le mot de passe d'un de vos comptes.
- Ne vous connectez jamais à des sites web bancaires ou importants (boîte de réception, documents personnels stockés en ligne…) via l'un de ces réseaux. N'achetez jamais quelque chose en ligne via ces derniers non plus. Attendez d'être sur un réseau fiable pour ce faire.
- N'installez jamais de mise à jour soi-disant obligatoire à partir de l'un de ces réseaux.

La clé USB piégée

Une clé USB piégée, qu’est-ce que c’est ?

Avez-vous déjà trouvé une clé USB ? Abstenez-vous de la connecter à votre ordinateur ! Celle-ci peut avoir été abandonnée dans le seul but de voler ou de **chiffrer vos données contre rançon.**

Comment vous protéger contre une clé USB piégée ?

En évitant tout simplement de la connecter à votre ordinateur. Rapportez-la plutôt au service des objets perdus de l’établissement dans lequel vous vous trouvez ou de votre ville.

Le « Virus »

Un virus, qu’est-ce que c’est ? Le virus est un bout de code de quelques octets dont la fonction est destructrice ou très gênante.

Son but est de détruire une partie ou toutes les données de l'ordinateur, ou encore de rendre inutilisables certaines fonctions du PC.

Il peut en outre ralentir certaines procédures.

De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants.

En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.

Le « Keylogger »

Un Keylogger, qu’est-ce que c’est ? C’est un « enregistreur de touches ».

Autrement dit, c'est un spyware capable de détecter les frappes sur le clavier de votre ordinateur et de les mémoriser.

Le tout, sans que vous le sachiez.

Il permet donc à des cybercriminels de mettre à jour vos identifiants et codes d'accès sur vos comptes privés ou professionnels.

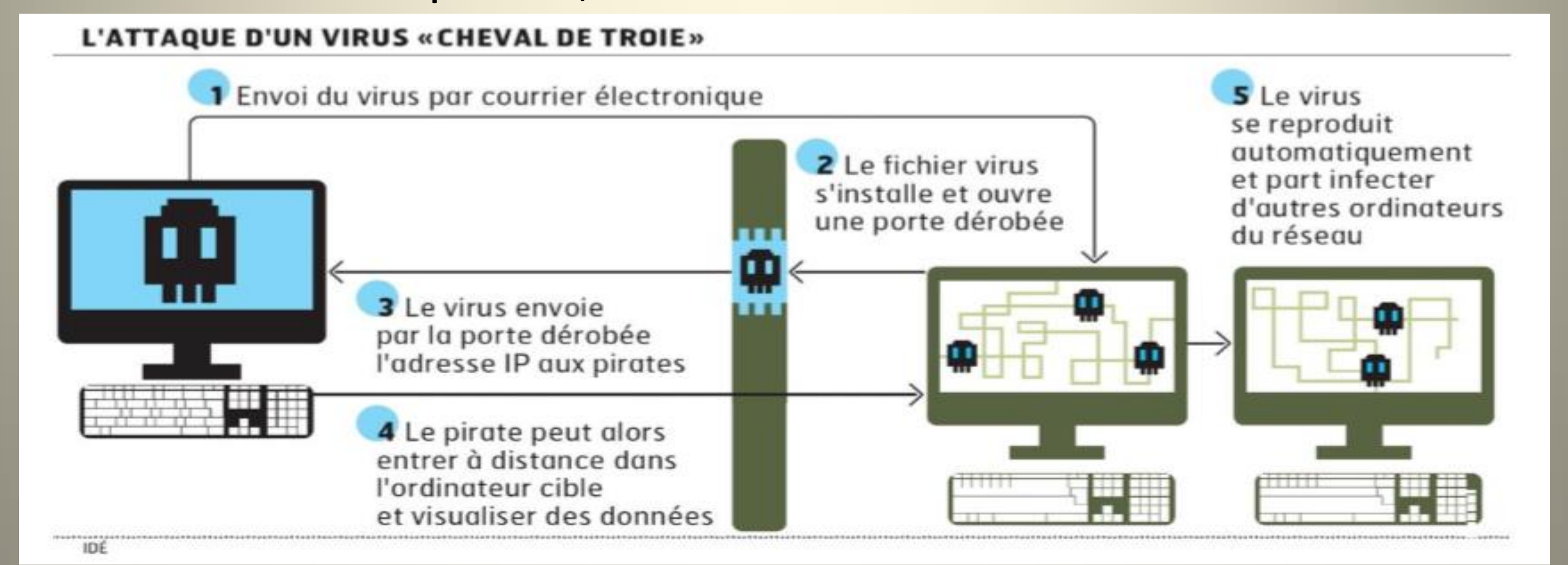
Les « Rootkits »

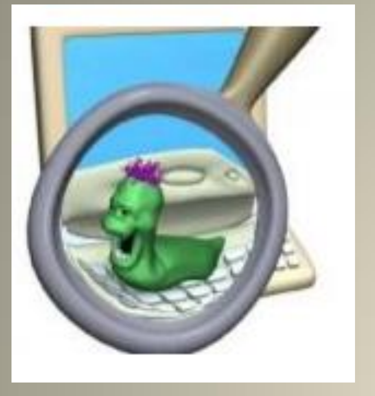
Un « rootkit », qu’est-ce que c’est ? C’est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible, à la différence d'autres logiciels malveillants.

Le « Cheval de Troie » (ou Trojan)

Un cheval de Troie, qu'est-ce que c'est ? C'est un programme installé discrètement par un pirate sur votre ordinateur simulant une certaine action, mais faisant tout autre chose en réalité.

Lorsque ce programme est lancé, il va causer des actions plus ou moins graves sur votre ordinateur, comme supprimer ou voler des mots de passe, envoyer des informations confidentielles au créateur du programme (données bancaires, N° de carte de crédit, etc.), formater votre disque dur, etc.





Le « Ver » (ou Worm en anglais)

Un ver (ou Worm), qu’est-ce que c’est ? : C’est un petit programme qui se copie d'ordinateur en ordinateur.

La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et ne peut donc pas l'infecter, il va simplement se copier d'ordinateur en ordinateur par l'intermédiaire d'un réseau comme Internet ou grâce aux échanges de périphériques comme les clés USB.

Le ver peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances des réseaux.

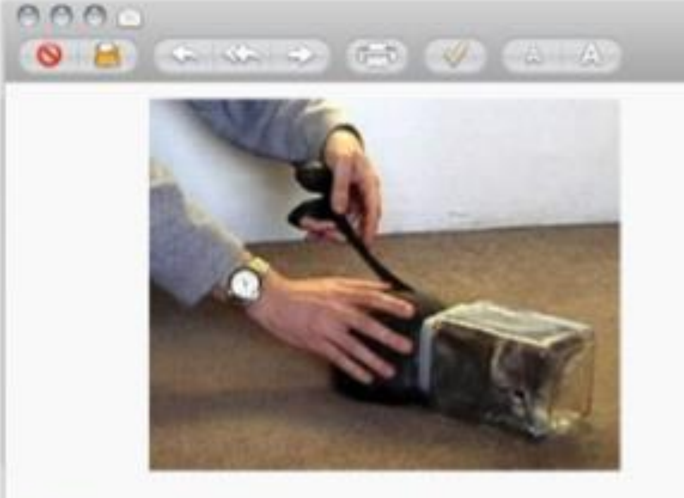
Comme un virus, le ver peut contenir une action nuisible qui peut être très grave comme le formatage de votre disque dur ou l'envoi de données confidentielles.

Le « Spyware » (ou Logiciel espion aussi appelé mouchard ou espiogiciel)

Un Spyware, qu'est-ce que c'est ? : C'est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et de transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.



Les hoax ou « faux virus » ou « fausse information » :



Voici un message que j'ai recu recemment :
CECI N'EST PAS UNE CONNERIE MAI UNE PETITION CONTRE UNE HORRIBLE MODE ASIATIQUE! PRENEZ 1 MINUTE MEME PAS POUR VOIR CETTE HORREUR ! SIGNEZ EN BAS ET FAITES PASSER, POUR UNE FOIS QUE CE N'EST PAS UNE DEBILITE !!!!!! REVOLTEZ VOUS

Bonjour!
A New York, il y a un magasin japonais qui vend des "bonsai-kittens". Ca a l'air amusant ?.....NON! Ces animaux (chats) sont enfermes dans un petit bocal. Leur urine et excrements sont evacues par des sondes. Ils les nourrissent par un genre de tube. Ils les nourrissent avec des produits chimiques pour que leurs os soient moux et flexibles pour que les chatons grandissent dans L'espace de la petite bouteille. Les animaux y restent aussi longtemps qu'ils sont en vie. Ils ne peuvent ni marcher , ni bouger, ou faire leur toilette. Les Bonsai-kittens sont entrain de devenir a la mode a New York et en Asie. Pour voir cette horreur : http://www.bonsaikitten.com S'il vous plait signez cette pÃÂ©tition contre ces tortures. Si vous recevez un E-mail avec plus de 500 signatures, s'il vous plait envoyez nous une copie a l'adresse: anacheca@hotmail.com. Cette petition sera envoyee aux organisations de protection des animaux aux E.-U. et au Mexique. Si vous envoyez ca a vos amis : utiliser un copier/coller dans un nouvel email pour que celui-ci reste lisible....
Transmis par Maya

Un hoax , qu'est-ce que c'est ? : Ces fausses alertes sont aussi sérieuses que les vrais virus, et malheureusement de plus en plus répandues. Elles font perdre du temps et peuvent générer un doute quant à la vérité ou non d'un message.

Si vous recevez un message du type : ***« si vous recevez un email avec comme sujet « machin », effacez-le, ne l'ouvrez pas, il formatera votre disque dur »,*** n'en tenez pas compte, supprimez le message et surtout ne l'envoyez pas à tout votre carnet d'adresses, cela ne fait qu'engorger le réseau. Pour savoir si une information est un Hoax ou non, on peut aller voir sur **« HoaxBuster »** et **« HoaxKiller »**.

On peut aussi chercher sur un moteur de recherche si on parle du sujet et voir si on peut faire confiance aux sites diffuseurs de l'information ou non…

Installer une bonne solution antivirus

Comme Roger, je me dois de vraiment vous conseiller d'utiliser la suite antivirus **« Sécurité Windows »** intégrée dans Windows 10. Ses mises à jour se font automatiquement. Notre avis commun est que cette suite, complète et gratuite, est très supérieure aux autres antivirus gratuits…

Le rôle de l'antivirus :

- Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les menaces les plus courantes présentes dans votre PC, : virus, rootkits, chevaux de Troie (ou Trojan), keyloggers… et de prendre des mesures pour les empêcher de nuire.
- Un antivirus doit savoir nous protéger **sans se faire remarquer**. **Il ne doit pas ralentir la machine.**
- Il faut être conscient qu'aucun antivirus n'est totalement infaillible et qu'il ne bloquera pas tous les dangers. Il conviendra donc de ne lui accorder qu'une confiance relative et de le compléter avec un antimalware, par exemple **« Malwarebytes »**...

Les techniques de détections des virus

Détection de la signature : On l'appelle aussi scan ou scanning. C'est la méthode la plus ancienne et la plus utilisée qui consiste à analyser le disque dur à la recherche de la signature du virus, présente dans la base de données du logiciel si celui ci est à jour et si il connaît ce virus.

Chaque virus a sa propre signature, qui doit être connue de l'antivirus. Cette méthode n'est pas efficace contre les nouveaux virus ou les virus dits polymorphes, dont la signature change à chaque réplication.

L'avantage de la technique du scan est qu'elle permet de détecter les virus avant leur exécution en mémoire, dès qu'ils sont stockés sur le disque et qu'une analyse est exécutée. Pour rester efficace, l'antivirus doit procéder à la mise à jour régulière de sa base de données antivirale. Une fréquence de mise à jour mensuelle est un minimum acceptable.

Le contrôle d'intégrité : Il permet de vérifier l'intégrité d'un fichier en vérifiant s’il a pas été modifié ou altéré au cours du temps. L'antivirus, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auxquels il aura associé des informations qui peuvent changer lorsqu’il est modifié (la taille, la date et heure de dernière modification, etc.). Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus recalcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé.

L'analyse heuristique : C'est la méthode la plus puissante car elle permet de détecter d'éventuels virus inconnus par votre antivirus. Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement). Elle provoque parfois de fausses alertes (Par ex. : ITunes a été un temps détecté comme virus par Avast).

Le comportement de l'antivirus :

L'antivirus surveille en permanence le comportement des logiciels actifs ***(s'il est en fonctionnement et que la protection automatique est activée).***

Il analyse tous les fichiers modifiés et créés.

En cas d'anomalie, il avertit l'utilisateur par un message explicite. Cette protection est indispensable lorsque vous surfez sur internet.

Lorsque l'antivirus a détecté un virus, il offre **trois possibilités** à l'utilisateur.

- **Réparer le fichier :** L'antivirus doit être capable de réparer un fichier atteint. Mais ce n'est pas toujours possible.
- **Supprimer le fichier :** Si l'antivirus n'est pas capable de supprimer le fichier, vous pouvez le supprimer manuellement.
- **Mise en quarantaine du fichier infecté :** C'est une solution d'attente. L'antivirus place le fichier dans un dossier sûr du disque dur.

Comment choisir un antivirus si l’on ne souhaite (quand même) pas utiliser « Sécurité Windows » de Windows 10 ?

Les logiciels gratuits que l’on trouve sur l’Internet ont l'avantage d'être assez légers pour ne pas ralentir les ordinateurs. Leur point faible est qu'ils ne protègent l'utilisateur que des attaques les plus courantes.

Cela oblige à rester très vigilant, notamment au niveau des e-mails, du streaming et des téléchargements.

Les suites payantes (Norton, BitDefender, Kaspersky, MacAfee…) proposent des boucliers plus complets, pour sécuriser les transactions financières, protéger contre le vol de données personnelles et l'usurpation d'identité.

Ils peuvent garantir la sécurité de plusieurs ordinateurs, ainsi que des tablettes et des téléphones portables.

Mais tout cela ne sert à rien si vous oubliez de les mettre à jour.

Voici une liste (non exhaustive) d'antivirus gratuits parmi les plus connus :

- « Sécurité Windows » (suite complète et efficace incluse dans Windows 10, anciennement « Centre de sécurité Windows ».
- Kaspersky Free (Interface en Français).
- Avast !
- Antivir.
- AVG Free Edition.
- Ad-Aware Antivirus Free
- …

Et pour ceux qui veulent à tout prix investir dans une suite antivirus payante :

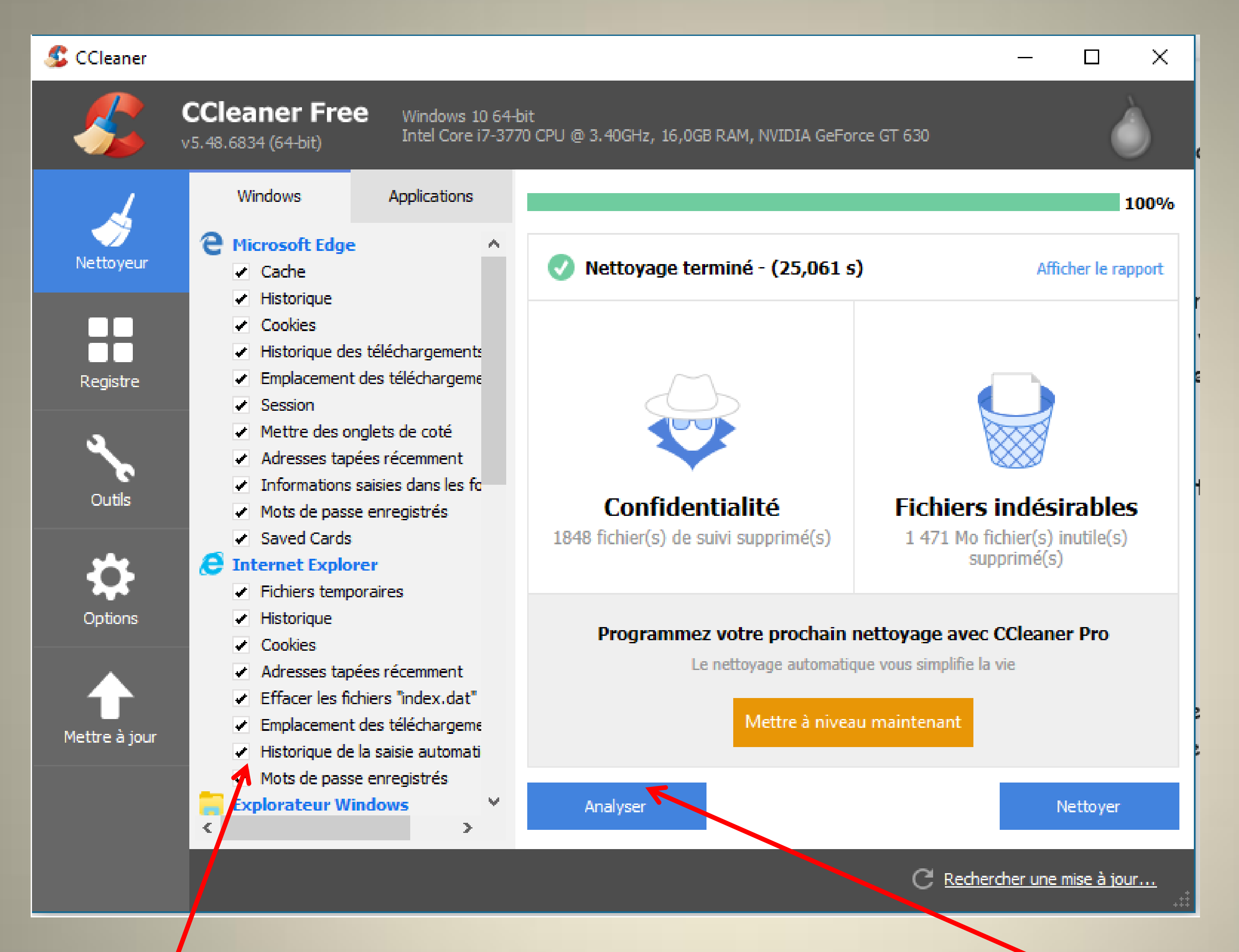
- **Norton by Symantec.**
- **Panda.**
- **Avira.**
- **Bitdefender.**
- **BullGuard**
- **McAfee**
- **et bien d’autres encore…**

Comment se protéger des malwares, spywares et autres parasites (en complément d'un bon antivirus) et renforcer la sécurité de tous vos équipements

Vos équipements sont associés automatiquement à des systèmes de défense qu'il convient de paramétrer pour limiter les attaques. Cette sécurité de base étant insuffisante, il est nécessaire d'installer des outils complémentaires à votre antivirus tels que CCleaner, Malwarebytes.

a) **CCleaner** est un utilitaire gratuit de nettoyage pour Windows permettant de récupérer de l'espace disque disponible, tout en allégeant le fonctionnement et le démarrage du système. Entièrement gratuit, il permet de vérifier et d'optimiser le système. **(Adresse de téléchargement : http://www.ccleaner.com/fr-fr/ccleaner/update?a=0&v=5.47.6716&t=4&au=1)**

Ccleaner s'installe comme n'importe quel logiciel. Vous double-cliquez sur le fichier téléchargé et cliquez sur « suivant » jusqu'à ce qu'il soit totalement installé. Pour le lancer, vous pouvez aller le chercher dans la liste de vos programmes, créer un raccourci sur le bureau ou placer son icone dans la barre des tâches.

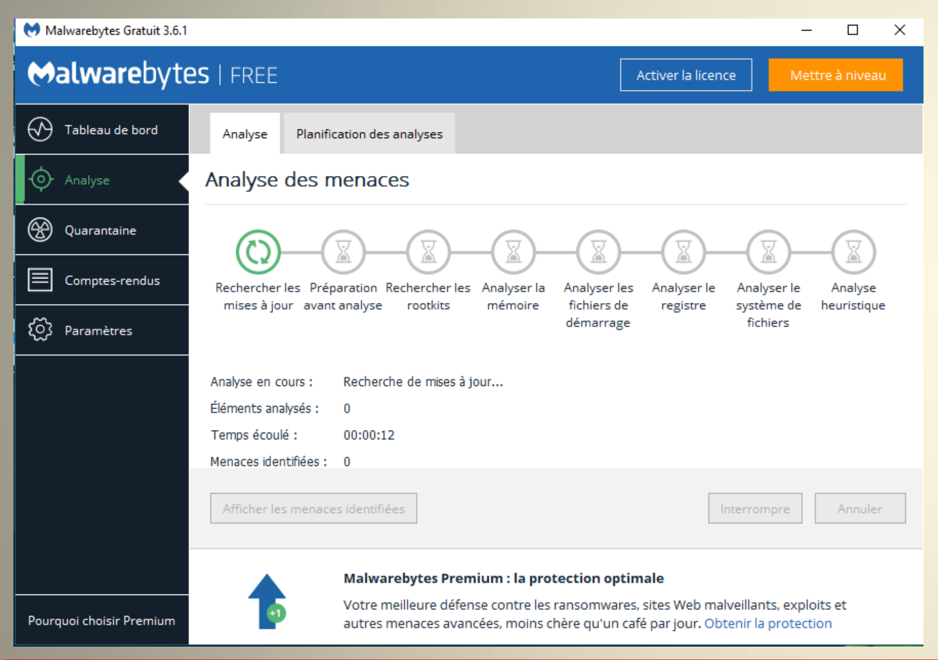


Cochez toutes les cases, puis cliquez sur « analyser ». Le processus est assez rapide (pas plus de 2min en général). Attention, cependant, rappelez-vous bien que **Ccleaner videra votre corbeille**. Fréquence : Tous les mois minimum.

b) Malwarebytes Anti-Malware est un logiciel gratuit et efficace qui protège votre système contre les logiciels malveillants (spywares, malwares, etc.).

Adresse de téléchargement : https://fr.malwarebytes.org/downloads/

Malwarebytes s'installe comme n'importe quel logiciel. Vous double-cliquez sur le fichier téléchargé et cliquez sur « suivant » jusqu'à ce qu'il soit totalement installé.



Pour le lancer, vous pouvez aller le chercher dans la liste de vos programmes, créer un raccourci sur le bureau ou placer son icone dans la barre des tâches. et cliquez ensuite sur « analyser maintenant ». L'analyse de votre ordinateur peut être plus ou moins rapide, mais en général ne dépasse pas 15min.

➔ MalwareBytes propose la version Pro à l'essai pour 15 jours. A la fin de période d'essai on peut revenir à la version gratuite. Ne pas accepter la version Pro pendant la période d'essai si l'on veut la version gratuite. Lorsque MalwareBytes assure la protection temps-réel pendant la période d'essai, il se substitue à « Sécurité Windows » ; à la fin de la période d'essai, « Sécurité Windows » reprend automatiquement le contrôle.

Limiter les intrusions sur vos appareils via les navigateurs web

Lorsque vous naviguez, les sites web peuvent installer des cookies sur votre disque dur et collecter vos données : **identifiants, mots de passe, sites web visités, etc.**

C'est ce qui vous permet de vous connecter automatiquement à vos sites préférés par exemple.

Les administrateurs de ces sites peuvent les utiliser pour faire de la **publicité intrusive**.

Attention, car les pirates peuvent également utiliser ces cookies pour capter vos données personnelles.

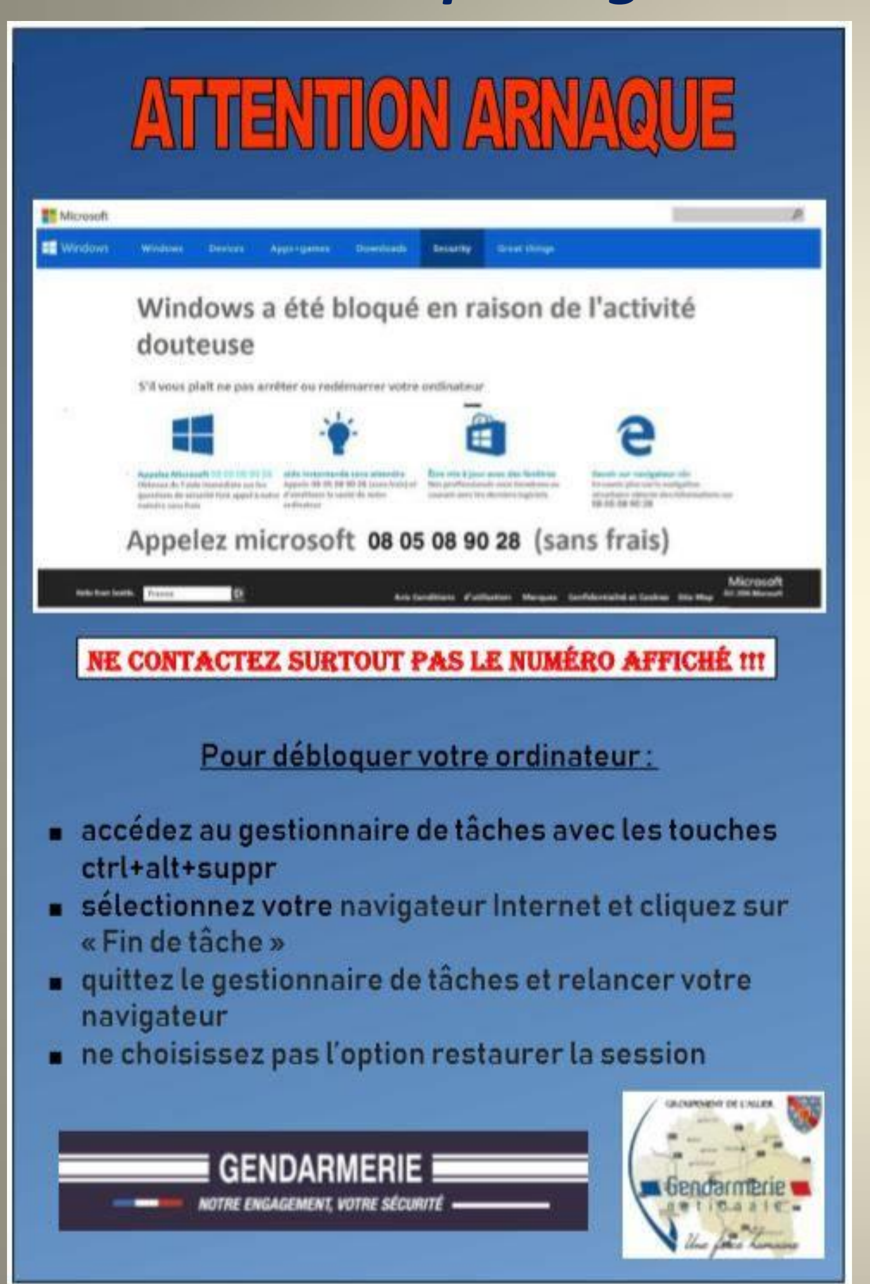
Pour mieux comprendre le fonctionnement des cookies et contrôler l'accès de certains sites à vos données, vous pouvez installer l'outil de visualisation de la CNIL **CookieViz** (à télécharger sur https://linc.cnil.fr/fr/cookieviz-une-dataviz-en-temps-reel-du-tracking-de-votre-navigation) qui identifie en temps réel ceux qui transmettent des informations vous concernant à d'autres sites.

N'oubliez pas de **mettre à jour votre système** et vos **applications** pour protéger vos équipements, car les versions non à jour sont plus vulnérables aux attaques.

Pour contrer ce fléau et sécuriser vos équipements, suivez ces quelques règles :

- ✓ Acceptez uniquement les cookies d'un site que vous fréquentez régulièrement.
- ✓ Décochez **« retenir les mots de passe »** dans votre navigateur et **changez-les** régulièrement.
- ✓ Vous pouvez les **crypter** grâce à un **gestionnaire de mots de passe** (KeePass ou dashlane par exemple).
- ✓ **Videz l'historique de votre navigateur** à la fin de chaque session.
- ✓ **Bloquez les publicités intempestives** qui peuvent installer des logiciels tiers à votre insu (bloqueur de publicité du navigateur ou logiciel de type AdBlock plus). Certains sites exigent leur désactivation, si l'on veut continuer, il faut désactiver le bloqueur de publicité.
- ✓ Empêchez les intrusions, la surveillance, les attaques de virus grâce à un logiciel **antivirus (à jour)** et au **pare feu** de votre système d'exploitation.
- ✓ Pour ne pas laisser de traces, vous pouvez **naviguer en mode privé**, sans laisser d'empreinte.

Actualité à partager - ARNAQUE AU BLOCAGE WINDOWS



Vous surfez tranquillement sur Internet, quand soudain une fenêtre «Windows» indiquant que votre ordinateur est bloqué s'affiche, avec une sirène et un message vocal.

Vous ne pouvez plus quitter la page.

Ne tombez pas dans le panneau, il s'agit d'une escroquerie destinée à vous soutirer de l'argent qui a déjà fait plusieurs victimes en Allier et dans toute la France.

Pour débloquer l'ordinateur, la fenêtre pop-up (voir l'image) précise qu'il faut contacter Microsoft en appelant le numéro de téléphone indiqué sur la page.

En le composant, l’internaute tombe sur un pseudo-technicien qui va prendre le contrôle à distance de son ordinateur pour installer des applications destinées à le ralentir. Pour résoudre le problème, l’escroc va ensuite demander à la victime de régler une somme conséquente soit plusieurs centaines d'euros.

Pas de panique, votre ordinateur n’est pas réellement bloqué.

Pour supprimer la page :

1. Accédez au gestionnaire de tâches avec les touches ctrl+alt+suppr ;
2. Sélectionnez votre navigateur Internet et cliquez sur « Fin de tâche » ;
3. Quittez le gestionnaire de tâches et relancer votre navigateur ;
4. Ne choisissez pas l’option restaurer la session.

Afin de prévenir les éventuelles attaques, **pensez à procéder aux mises à jour des logiciels et anti-virus.** Vous pouvez également installer un **bloqueur de pop-up (AdBlock, uBlock Origin, ...)** qui évite l'ouverture de ce type de fenêtre.

A l’issue, **signalez l’escroquerie** :

- soit sur le site du gouvernement dédié aux contenus illicites, www.internet-signalement.gouv.fr à la rubrique escroquerie ;
- soit par téléphone via le numéro vert gratuit mis en place par le gouvernement : **0 805 805 817**. »

Boîte mail piratée : comment vérifier et comment y remédier?

Piratage de boîte e-mail : Chacune, chacun d'entre nous est susceptible, par le biais d'Internet, d'accéder à des applications pouvant contenir des informations personnelles, confidentielles et sensibles.

Bien sûr celles-ci sont censées être protégées par des mots de passe, mais par faiblesse de ces derniers ou par « dextérité » de certains hackers, il peut arriver que notre **compte soit piraté**.

Nous allons voir comment nous en rendre compte, sur les principales plateformes de mail, et comment nous pourrons y remédier.

Tout d'abord, recherchez votre adresse IP (1). Cet identifiant sur le réseau vous permettra de repérer si quelqu'un d'autre que vous se connecte sur votre compte. Pour ce faire, aller sur un site tel que **« mon-ip.com »** (http://www.mon-ip.com/) pour récupérer votre adresse IP.

Attention, les fournisseurs d'accès fournissent des adresses IP dynamiques, qui sont réinitialisées à chaque connexion. Il faut donc la vérifier à chaque connexion. Si l'on veut une adresse IP fixe, il faut le demander à son fournisseur d'accès, mais elle sera payante.

(1) Adresse IP (Internet Protocol) : Numéro unique permettant à un ordinateur de communiquer dans un réseau.

Comment détecter si ma boîte e-mail est piratée ?

Yahoo Mail :

Connectez-vous à votre compte, cliquez sur la roue dentée à droite de votre nom puis cliquez sur **« Paramètres du Compte »**.

Une nouvelle page s’affiche, sélectionnez alors **« Activité Récente »**.

L’ensemble des connexions, leur adresse IP d’origine, ainsi que le type d’appareils utilisés s’affiche dans une liste.

Vérifiez que vous êtes bien l’auteur de ces connexions.

Dans le cas contraire votre **boîte mail est piratée**!

Outlook :

Après vous être connecté, cliquez sur votre nom puis sur « Paramètres du compte ». Sélectionnez également **« Activités Récentes »** pour afficher la liste des derniers accès à votre compte, dans la section **« Sécurité et confidentialité »**.

Vous vous rendrez vite compte du **piratage** de votre **boîte mail** par les activités anormales listées à cet emplacement.

Gmail :

Après avoir renseigné les paramètres de votre compte, cliquez sur votre « avatar » en haut à droite puis choisissez **« Compte »** en dessous de votre adresse mail.

Descendez dans la page, à la rubrique **« Activité Récente »** vous trouverez la ligne **« Appareil »**.

En cliquant dessus vous pourrez voir toutes les connexions effectuées sur votre compte.

Normalement vous devriez reconnaître les lieux de connexion…

Si une connexion est réalisée à Turin alors que vous êtes sur les bords de Seine, il y a un problème.

Que faire en cas de suspicion de piratage de sa boîte mail ?

Pas de panique, ***vous avez encore les clés si vous avez réussi à vous connecter.***

Deux étapes majeures sont à réaliser :

1°) **Vérifier** qu'il n'y a **aucune redirection** de **votre compte mail** vers un compte autre, celui d'un éventuel pirate :

→ Sur **Yahoo Mail** il suffit de se rendre sur **« Paramètres »** puis de cliquer sur **« Comptes »** et de vérifier qu'aucun compte n'est défini dans l'espace **« Envoyer et recevoir des mails dans des comptes extérieurs »**.

→ Sur **Gmail** et **autres**, la démarche est sensiblement **équivalente**.

2°) **Changer** votre **mot de passe**, pour empêcher toute intrusion future.

Prenez soin de le choisir suffisamment complexe, mais mémorisable facilement pour vous.

Un combo **« mot de passe de base »** + **« nom du site »** + **variante chiffrée** + **caractères spéciaux** devrait suffire !

➔ Sur **Yahoo Mail**, c'est également dans **« Paramètres du compte »** puis **« Sécurité du compte »** et enfin **« Modifier le mot de passe »**.

➔ Sur **Gmail** et **autres**, la démarche est encore une fois sensiblement équivalente.

Une fois le mot de passe changé, **n'oubliez** pas de **redéfinir votre connexion** à votre email **sur votre smartphone** en renseignant le nouveau de mot de passe, sinon vous allez devoir attendre longtemps pour recevoir vos mails dessus !

Prenez de bonnes habitudes pour protéger votre boîte mail :

- ✓ Bien vérifier l’origine du mail reçu avant de cliquer sur une pièce jointe.
- ✓ Ne stockez jamais de mots de passe dans votre boîte mail.
- ✓ A chaque fois que vous recevez un mot de passe par e-mail, changez-le
- ✓ Notez vos mots de passe dans un endroit sécurisé.
- ✓ Établissez une règle personnelle pour avoir un mot de passe différent sur chaque site internet et facile à mémoriser.
- ✓ Vérifiez toujours avant de saisir vos identifiants que vous êtes sur un site de confiance.
- ✓ Éventuellement : investissez dans un gestionnaire de mots de passe…

Mots de passe : 4 questions essentielles pour bien les choisir

En plus d’être à la fois robuste et facile à retenir, un bon mot de passe ne doit protéger qu’un seul accès.

Quelques conseils pratiques pour faire les bons choix et obtenir un niveau de sécurité optimal.

Malgré l’apparition de nouvelles technologies pouvant faire office de serrure électronique, les mots de passe restent encore très utilisés : que ce soit par les entreprises, les e-commerçants ou encore les services publics en ligne,

De quoi nous obliger à en créer régulièrement, à les changer de temps en temps et surtout à les retenir.

Un exercice qui peut se transformer en véritable challenge!

Voici quelques conseils pour le relever.

1/ Puis-je utiliser le même mot de passe pour plusieurs comptes ?

La tentation est forte, bien sûr, mais c'est vivement déconseillé : Si, un jour, votre mot de passe est découvert par un hacker, ce dernier ne manquera pas de l'utiliser sur d'autres comptes vous appartenant (messageries électroniques, sites e-commerce, réseaux sociaux…) et pourra ainsi prendre la main, en quelques clics seulement, sur ces derniers.

2/ Dois-je choisir des chiffres et des lettres n'ayant aucun sens ?

Un mot de passe compliqué – composé de différents types de signes (minuscules, majuscules, chiffres, ponctuations, caractères spéciaux…) et n'ayant aucun sens – résistera plus longtemps à l'attaque d'un hacker qu'un simple mot ou qu'une suite logique de chiffres ou de lettres.

Mais il est difficile de se souvenir d'un mot de passe pareil ! Il est donc préférable d'opter pour des mots de passe plus longs, mais ayant néanmoins du sens pour vous comme une suite de mots ou une phase complète. Par exemple ? « À-12h30,-chaque-jour,-je-prends-ma-pause-déjeuner-! » est un mot de passe à la fois facile à retenir et très robuste.

3/ Suis-je obligé(e) de changer régulièrement de mot de passe ?

Les responsables informatiques sont, en effet, nombreux à le préconiser : tous les 3 ou 6 mois, en fonction de la sensibilité des données abritées par le compte.

Néanmoins, certaines études menées sur le sujet constatent, à juste titre, que cela complique la vie des utilisateurs…

Ces derniers pouvant ainsi être tentés de simplifier leurs mots de passe ou à ne modifier que très faiblement le mot de passe devant être remplacé (par exemple, en y ajoutant un chiffre) pour s’en souvenir plus facilement.

Or, à choisir, c’est la robustesse du mot de passe qui doit être privilégiée, et non son rythme de changement.

4/ Et si j'optais pour un gestionnaire de mots de passe ?

Un gestionnaire de mot de passe est un logiciel administrant une base de données très sécurisée.

Sa mission ? Stocker vos identifiants, ainsi que tous les mots de passe associés, pour vous permettre de vous connecter sur les sites sécurisés auxquels vous êtes abonnés.

Souvent accessibles en ligne, permettant à l'utilisateur de s'en servir sur n'importe quel équipement (ordinateur, tablette, smartphone), ces outils sont fréquemment dotés d'un générateur de mot de passe offrant un niveau de sécurité élevé.

Par ailleurs, si la plupart des navigateurs web intègrent des systèmes de mémorisation des mots de passe, il faut savoir que ces outils restent très rudimentaires. Il convient ainsi de leur préférer des logiciels spécifiques, souvent proposés gratuitement ou à des tarifs peu onéreux, sur les différentes plates-formes en ligne (App Store, Google Play, Microsoft Store…). En utilisant un logiciel gestionnaire de mots de passe, vous n'aurez plus qu'un seul mot de passe à retenir : celui qui permet de l'utiliser. Il va sans dire qu'il conviendra de le choisir avec le plus grand soin…

Vie privée et réseaux sociaux

La frontière entre vie privée et vie publique n'a jamais été aussi mince sur le net.

Pour éviter que votre intimité ne se trouve compromise, il vous appartient d'exercer une vigilance constante.

En effet, la majorité des fuites d'informations privées sur le net provient de négligences ou de manque de connaissances des internautes.

Les bonnes pratiques de navigation sur les réseaux sociaux :

Lorsque l'on parle de **protection de la vie privée**, on pense désormais en premier lieu aux réseaux sociaux.

Vous pourriez supposer que le principe de base de ce type de plateforme est justement de partager son intimité avec vos amis.

Cependant, il vous faut être très vigilant sur vos partages.

Sur Twitter : vous pouvez décider de paramétrer votre compte en mode privé : Seuls vos followers que vous validerez pourront avoir accès à vos tweets.

Sur Facebook : Il est peu recommandé de divulguer trop d'informations personnelles sensibles (date ou lieu de naissance, numéro de téléphone ou adresse de domicile précise) sur ce réseau.

Lorsque vous partagez une photo, un statut, vérifiez bien systématiquement avec qui vous le faites.

Par défaut, vos publications sont accessibles à tous.

Il vous appartient de maîtriser ce paramètre : ***Toujours passer par les options de compte Facebook pour régler la confidentialité de vos informations.***

Il est recommandé de **ne pas autoriser les personnes ne figurant pas dans votre liste d'amis** à voir vos informations et vos posts.

Préserver sa vie privée sur Internet : Disparaître des résultats des moteurs de recherches ou « Droit à l'oubli »



Depuis 2014, la Cour Européenne de Justice a décidé que les utilisateurs disposeraient désormais d'un *« droit à l'oubli »* ***(cf. https://fr.wikisource.org/wiki/Charte_du_droit_à_l'oubli_dans_les_sites_collaboratifs_et_les_moteurs_de_recherche)*****.**

Les fournisseurs de moteurs de recherche **comme Google** sont tenus de proposer un moyen de supprimer de leurs listes de résultats les liens vers des pages Web contenant des données sensibles et personnelles.

Via un formulaire en ligne ***(https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636759960369937559-816893273&rd=1)***, tout citoyen européen peut désormais demander la suppression de son nom dans les résultats de recherche de Google.

Sites d'informations utiles **:**

- ✓ https://www.internet-signalement.gouv.fr/PortailWeb/planets/ConseilsProteger.action
- ✓ https://www.economie.gouv.fr/entreprises/nouveau-site-web-cybermalveillance
- ✓ http://www.commentcamarche.net/faq/8934-securisation-de-son-pc#antivirus-gratuit
- ✓ https://lecrabeinfo.net/comment-proteger-et-securiser-son-pc.html
- ✓ https://www.youtube.com/user/LACNIL/videos
- ✓ https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/cybercriminalite/actualite-846861-cybersecurite-2018-quelles-5-grandes-menaces.html?utm_source=dlvr.it&utm_medium=facebook

Maintenant,
vous savez vous protéger
et éviter les écueils
alors bon surf
sur la grande toile